COMMON DIRECTORY SERVICES AND PROCEDURES

ACP 133 Edition B

March 2000

(Reverse Blank)

replace this page with a blank one

FOREWORD

1. ACP 133, COMMON DIRECTORY SERVICES AND PROCEDURES, is an UNCLASSIFIED Allied Communication Publication (ACP). Periodic accounting of this publication is not required.

2. ACP 133 will be effective for National, Service, or Allied use when directed by the appropriate Implementing Agency; refer to the National Letter of Promulgation (LOP).

3. This publication contains Allied military information and is furnished for official purposes only.

4. This publication is not releasable without prior approval from the United States Military Communications-Electronic Board (USMCEB).

5. It is permitted to copy or make extracts from this publication without consent of the Authorizing Agency.

replace this page with a blank one

UK NATIONAL LETTER OF PROMULGATION

The purpose of this UK National letter of promulgation is to implement ACP 133 (B) within the Armed Forces of United Kingdom of Great Britain and Northern Ireland.

1. ACP 133 (B) DIRECTORY SERVICES, is an Unclassified non-registered Allied Communications Publication (ACP).

2. ACP 133 (B) is effective on receipt and replaces ACP 133 (A) which should be destroyed in accordance with local security instructions.

3. Comments or recommendations should be forwarded through the chain of command to the Defence Communications Procedures Branch (DCPB), Room 336, Northumberland House, Northumberland Avenue, London WCN 5BP.

4. Report any loss or compromise of this publication through the appropriate chain of command, in accordance with current Services requirements.

5. Extracts may be taken from this publication.

By Command of the Defence Council

Permanent Under Secretary

replace this page with a blank one

RECORD OF CHANGES AND CORRECTIONS

Enter Change or Correction in Appropriate Column

Identification of Change or Correction; Reg. No. (if any) and date of same		Date Entered	By whom entered (Signature; rank, grade, or rate; name of command)
Change	Correction		
205 b		September 1999	ACP 133 Task Force
219, Table 2-3		September 1999	ACP 133 Task Force
227		September 1999	ACP 133 Task Force
303 j		September 1999	ACP 133 Task Force
305		September 1999	ACP 133 Task Force
307 a, b		September 1999	ACP 133 Task Force
308 c		September 1999	ACP 133 Task Force
308 e		September 1999	ACP 133 Task Force
310 a, b, c, e, f, i, j, k,		September 1999	ACP 133 Task Force
l, p, g, r		September 1999	ACP 133 Task Force
311 m, p		September 1999	ACP 133 Task Force
Tables 3-1, 3-2, 3-3, 3-4, 3-5, 3-7, 3-9, 3-10, 3-11, 3-12, 3-13, 3-15, 3-16, 3-18, 3-19		September 1999	ACP 133 Task Force
Annex A, 1 r, s, t, u, v, w, y, bb, dd, hh		September 1999	ACP 133 Task Force
Annex A, 1, renumbered ee - iii		September 1999	ACP 133 Task Force
Annex A, 2 b, d		September 1999	ACP 133 Task Force
Annex A, 2, renumbered c		September 1999	ACP 133 Task Force
Annex A, 4		September 1999	ACP 133 Task Force
Annex A, 5		September 1999	ACP 133 Task Force
Annex B, 1		September 1999	ACP 133 Task Force
Annex B, 1 c		September 1999	ACP 133 Task Force
Annex B, 3 b, e, i, j, n, o, p, q		September 1999	ACP 133 Task Force
Annex B, 4 b, c		September 1999	ACP 133 Task Force
Annex B, 5 a, b, c, i, j, k, p, q		September 1999	ACP 133 Task Force
Annex B, 5, renumbered l - w		September 1999	ACP 133 Task Force
Annex B, 5 l, m, n, o, p (1), r, s, t, u, v, w		September 1999	ACP 133 Task Force

RECORD OF CHANGES AND CORRECTIONS

Enter Change or Correction in Appropriate Column

Identification of Change or Correction; Reg. No. (if any) and date of same		Date Entered	By whom entered (Signature; rank, grade, or rate; name of command)
Change	Correction		
Annex B, 6 a		September 1999	ACP 133 Task Force
Annex B, 7		September 1999	ACP 133 Task Force
Annex B, 7 a, b, c, d, e, l, m		September 1999	ACP 133 Task Force
Annex B, 7, renumbered f - l, n - o		September 1999	ACP 133 Task Force
Annex B, 7 d (1), f, g, h, i, j, k, l (1), n		September 1999	ACP 133 Task Force
Annex B, 8 c		September 1999	ACP 133 Task Force
Annex B, 9		September 1999	ACP 133 Task Force
Annex B, 11 a, e		September 1999	ACP 133 Task Force
Annex B, 12 a, d, g, j, l, p, s, t, v, z, cc, ee, hh, ii, ll, nn,		September 1999	ACP 133 Task Force
Annex B, 12 cc (2)		September 1999	ACP 133 Task Force
Annex B, 12 ee (2)		September 1999	ACP 133 Task Force
Annex B, 15		September 1999	ACP 133 Task Force
Annex B, 40 a		September 1999	ACP 133 Task Force
Annex B, 45		September 1999	ACP 133 Task Force
Annex B, renumbered 46 -132		September 1999	ACP 133 Task Force
Annex B, 47		September 1999	ACP 133 Task Force
Annex B, 52 a		September 1999	ACP 133 Task Force
Annex B, 54		September 1999	ACP 133 Task Force
Annex B, 84		September 1999	ACP 133 Task Force
Annex B, 86 a		September 1999	ACP 133 Task Force
Annex B, 93 a		September 1999	ACP 133 Task Force
Annex B, 133		September 1999	ACP 133 Task Force
Renumber 134 - 201		September 1999	ACP 133 Task Force
Annex B, 160 a		September 1999	ACP 133 Task Force
Annex B, 181 a		September 1999	ACP 133 Task Force
Annex B, 187 b		September 1999	ACP 133 Task Force
Annex B, 187, renumbered c - f		September 1999	ACP 133 Task Force

RECORD OF CHANGES AND CORRECTIONS

Enter Change or Correction in Appropriate Column

Identification of Change or Correction; Reg. No. (if any) and date of same		Date Entered	By whom entered (Signature; rank, grade, or rate; name of command)
Change	Correction		
Annex B, 190 b (3)		September 1999	ACP 133 Task Force
Annex B, 197		September 1999	ACP 133 Task Force
Annex B, 197, module name and oid		September 1999	ACP 133 Task Force
Annex B, 197, Imports		September 1999	ACP 133 Task Force
Annex B, 197 a, c, d, h, i, k, l, m, n, o, s, t, w, x, y		September 1999	ACP 133 Task Force
Annex B, 199, module name and oid		September 1999	ACP 133 Task Force
Annex B, 199, Imports		September 1999	ACP 133 Task Force
Annex B, 199 a (9), (15)		September 1999	ACP 133 Task Force
Annex B, 199 a, renumbered (10) - (14), (16) - (21)		September 1999	ACP 133 Task Force
Annex B, 199 b (7)		September 1999	ACP 133 Task Force
Annex B, 199 b, renumbered (8)		September 1999	ACP 133 Task Force
Annex B, 199 c (66)		September 1999	ACP 133 Task Force
Annex B, 199 c, renumbered (67) - (92)		September 1999	ACP 133 Task Force
Annex B, 199 c (84)		September 1999	ACP 133 Task Force
Annex B, 199 e (11), (24)		September 1999	ACP 133 Task Force
Annex B, 199 e, renumbered (12) - (23), (25) - (30)		September 1999	ACP 133 Task Force
Annex B, 199 g		September 1999	ACP 133 Task Force
Annex B, 201, module name and oid		September 1999	ACP 133 Task Force
Annex B, 201 b		September 1999	ACP 133 Task Force
Annex B, 201, renumbered c - f		September 1999	ACP 133 Task Force

RECORD OF CHANGES AND CORRECTIONS

Enter Change or Correction in Appropriate Column

Identification of Change or Correction; Reg. No. (if any) and date of same		Date Entered	By whom entered (Signature; rank, grade, or rate; name of command)
Change	Correction		
Tables B-25, B-31, B-47		September 1999	ACP 133 Task Force
Renumbered Tables B-26 to B-30, B-32 to B-42, B-45, B-48, B-50to B-52		September 1999	ACP 133 Task Force
Table B-38		September 1999	ACP 133 Task Force
Table B-43, Table B-44		September 1999	ACP 133 Task Force
Table B-49		September 1999	ACP 133 Task Force
Figure B-1		September 1999	ACP 133 Task Force
Figure B-2		September 1999	ACP 133 Task Force
Annex D, 3 i		September 1999	ACP 133 Task Force
Annex D, 3, renumber j - n		September 1999	ACP 133 Task Force
Annex D, 3 j, k, l, m, n,		September 1999	ACP 133 Task Force
Annex D, 4 a (2), (3), (4), (5), (6), (7), (8), (9), (10), (11), (12)		September 1999	ACP 133 Task Force
Annex D, 4 b (2), (3), (4), (5), (6), (7), (8),(9)		September 1999	ACP 133 Task Force
Annex D, 4 c (2), (3), (5), (7)		September 1999	ACP 133 Task Force
Annex D, 4 d (2), (3), (6)		September 1999	ACP 133 Task Force
Annex D, 5 a, b, c		September 1999	ACP 133 Task Force
Annex D, 6 a, b, c, d, e, f, g, h, i, j, k, l		September 1999	ACP 133 Task Force
Annex D, 7 a, b, c, d, e, f, g		September 1999	ACP 133 Task Force
Annex D, 8		September 1999	ACP 133 Task Force
Annex D, 9		September 1999	ACP 133 Task Force
Annex D, 10		September 1999	ACP 133 Task Force
Table D-7		September 1999	ACP 133 Task Force
Table D-9		September 1999	ACP 133 Task Force
Table D-11		September 1999	ACP 133 Task Force

RECORD OF CHANGES AND CORRECTIONS

Enter Change or Correction in Appropriate Column

Identification of Change or Correction; Reg. No. (if any) and date of same		Date Entered	By whom entered (Signature; rank, grade, or rate; name of command)
Change	Correction		
Table D-12		September 1999	ACP 133 Task Force
Renumber Tables D-13 to D-17		September 1999	ACP 133 Task Force
Table D-14		September 1999	ACP 133 Task Force
Table D-16		September 1999	ACP 133 Task Force
Table D-18		September 1999	ACP 133 Task Force
Table D-19		September 1999	ACP 133 Task Force
Table D-20		September 1999	ACP 133 Task Force
Table D-21		September 1999	ACP 133 Task Force
Table D-22		September 1999	ACP 133 Task Force
Table D-23		September 1999	ACP 133 Task Force
Table D-24		September 1999	ACP 133 Task Force
Table D-25		September 1999	ACP 133 Task Force
Table D-26		September 1999	ACP 133 Task Force
Renumber Tables D-27 to D-30		September 1999	ACP 133 Task Force
Table D-30		September 1999	ACP 133 Task Force
Table D-31		September 1999	ACP 133 Task Force
Table D-32		September 1999	ACP 133 Task Force
Table D-33		September 1999	ACP 133 Task Force
Table D-34		September 1999	ACP 133 Task Force
Table D-35		September 1999	ACP 133 Task Force
Renumber Tables D-36 to D-50		September 1999	ACP 133 Task Force
Table D-46		September 1999	ACP 133 Task Force
Table D-53		September 1999	ACP 133 Task Force
Table D-54		September 1999	ACP 133 Task Force
Table D-55		September 1999	ACP 133 Task Force
Table D-56		September 1999	ACP 133 Task Force
Table D-57		September 1999	ACP 133 Task Force
Table D-58		September 1999	ACP 133 Task Force
Table D-59		September 1999	ACP 133 Task Force
Table D-60		September 1999	ACP 133 Task Force
Table D-61		September 1999	ACP 133 Task Force

RECORD OF CHANGES AND CORRECTIONS

Enter Change or Correction in Appropriate Column

Identification of Change or Correction; Reg. No. (if any) and date of same		Date Entered	By whom entered (Signature; rank, grade, or rate; name of command)
Change	Correction		
Table D-62		September 1999	ACP 133 Task Force
Table D-63		September 1999	ACP 133 Task Force
Table D-64		September 1999	ACP 133 Task Force
Table D-65		September 1999	ACP 133 Task Force
Table D-66		September 1999	ACP 133 Task Force
Annex D, Appendix 1		September 1999	ACP 133 Task Force
Annex G		September 1999	ACP 133 Task Force
Title Page, Headers, & Footers		March 2000	ACP 133 Task Force
101 e		March 2000	ACP 133 Task Force
211 b		March 2000	ACP 133 Task Force
301 a (1) & (2)		March 2000	ACP 133 Task Force
303 j (1) (b)		March 2000	ACP 133 Task Force
305		March 2000	ACP 133 Task Force
307 a & b		March 2000	ACP 133 Task Force
Figures 3-4 to 3-6		March 2000	ACP 133 Task Force
309 f, g, h, & i		March 2000	ACP 133 Task Force
Insert new 309 i and renumber next subparagraph.		March 2000	ACP 133 Task Force
310 e, f, h, i, j, k, l, p, q, & r		March 2000	ACP 133 Task Force
311 a, m, & p		March 2000	ACP 133 Task Force
Insert new 311 d and renumber subsequent subparagraphs.		March 2000	ACP 133 Task Force
Tables 3-1 to 3-21		March 2000	ACP 133 Task Force
Annex A 5 b		March 2000	ACP 133 Task Force
Annex B 1 a		March 2000	ACP 133 Task Force
Annex B 3 e, n, o, p, & q		March 2000	ACP 133 Task Force
Annex B 4 c		March 2000	ACP 133 Task Force
Annex B 5 a, l, m, r, s, & t		March 2000	ACP 133 Task Force

RECORD OF CHANGES AND CORRECTIONS

Enter Change or Correction in Appropriate Column

Identification of Change or Correction; Reg. No. (if any) and date of same		Date Entered	By whom entered (Signature; rank, grade, or rate; name of command)
Change	Correction		
Insert new 5 c, d, & i into Annex B and renumber subsequent subparagraphs.		March 2000	ACP 133 Task Force
Insert new Table B-17, Table B-18 & Table B-23 and renumber subsequent tables (throughout Annex B). Also, correct references to tables.		March 2000	ACP 133 Task Force
Table B-41 (new #)		March 2000	ACP 133 Task Force
Annex B 7 and 7 e, k, & o		March 2000	ACP 133 Task Force
Annex B 8 d		March 2000	ACP 133 Task Force
Annex B 9		March 2000	ACP 133 Task Force
Annex B 11 a, e, &f		March 2000	ACP 133 Task Force
Table B-54		March 2000	ACP 133 Task Force
Annex B 12 d (3), g, j (1), w, x, y, z, aa, cc, dd (3), ee, ff (3), ii, kk, & mm (1)		March 2000	ACP 133 Task Force
Insert a new subparagraph 12 m into Annex B and renumber subsequent subparagraphs		March 2000	ACP 133 Task Force
Figure B-1 and Figure B-2		March 2000	ACP 133 Task Force
Annex B 16 a and add 16 b		March 2000	ACP 133 Task Force
Annex B 19 b		March 2000	ACP 133 Task Force
Annex B 23 a		March 2000	ACP 133 Task Force
37 a		March 2000	ACP 133 Task Force
40 a		March 2000	ACP 133 Task Force

RECORD OF CHANGES AND CORRECTIONS

Enter Change or Correction in Appropriate Column

Identification of Change or Correction; Reg. No. (if any) and date of same		Date Entered	By whom entered (Signature; rank, grade, or rate; name of command)
Change	Correction		
41 a		March 2000	ACP 133 Task Force
59 a		March 2000	ACP 133 Task Force
84 b		March 2000	ACP 133 Task Force
94 a		March 2000	ACP 133 Task Force
103 a		March 2000	ACP 133 Task Force
117 a		March 2000	ACP 133 Task Force
120 a		March 2000	ACP 133 Task Force
121 b		March 2000	ACP 133 Task Force
124 a		March 2000	ACP 133 Task Force
160 a		March 2000	ACP 133 Task Force
196 a		March 2000	ACP 133 Task Force
197, 197 k, l, m, n, u, & v		March 2000	ACP 133 Task Force
199 c 75, 85, 90, & 92		March 2000	ACP 133 Task Force
199 f, g		March 2000	ACP 133 Task Force
Insert new paragraphs 21, 22, 23, 28, 57, 70, 176, 184, 197 o, 199 a (1) (2), & (7); 199 c (4), (5), (11), (29), (36), (91) & (93); 199 e (1), (2), & (8) into Annex B and renumber subsequent paragraphs.		March 2000	ACP 133 Task Force
Annex D Table of Contents added		March 2000	ACP 133 Task Force
Annex D 1 a		March 2000	ACP 133 Task Force
Table D-7		March 2000	ACP 133 Task Force
Table D-19		March 2000	ACP 133 Task Force
Table D-21		March 2000	ACP 133 Task Force
Table D-30		March 2000	ACP 133 Task Force

RECORD OF CHANGES AND CORRECTIONS

Enter Change or Correction in Appropriate Column

Identification of Change or Correction; Reg. No. (if any) and date of same		Date Entered	By whom entered (Signature; rank, grade, or rate; name of command)
Change	Correction		
Insert a new level of subparagraphs (a - d) below Annex D 6 and renumber existing subparagraphs at the next lower level.		March 2000	ACP 133 Task Force
Table D-42		March 2000	ACP 133 Task Force
Table D-43		March 2000	ACP 133 Task Force
Table D-45		March 2000	ACP 133 Task Force
Table D-49		March 2000	ACP 133 Task Force
Table D-51		March 2000	ACP 133 Task Force
Table D-61		March 2000	ACP 133 Task Force
Insert a new Table D-44 and subparagraph 6 a (4) into Annex D. Renumber subsequent tables and correct references to tables.		March 2000	ACP 133 Task Force
Annex G		March 2000	ACP 133 Task Force

RECORD OF CHANGES AND CORRECTIONS

Enter Change or Correction in Appropriate Column

Identification of Change or Correction; Reg. No. (if any) and date of same		Date Entered	By whom entered (Signature; rank, grade, or rate; name of command)
Change	Correction		

RECORD OF PAGES CHECKED*

Date Checked	By Whom Checked (Signature and Rank)	Date Checked	By Whom Checked (Signature and Rank)

*THIS PAGE NOT APPLICABLE TO US HOLDERS

NOTE: To meet local requirements, this page may be replaced when all entries are filled. The publication holder is to arrange local reproduction, and certify the replacement pages as a “true copy”. The original page numbers are to be allocated to the copy. Superseded pages should then be destroyed in accordance with applicable National instructions.

RECORD OF PAGES CHECKED*

Date Checked	By Whom Checked (Signature and Rank)	Date Checked	By Whom Checked (Signature and Rank)

*THIS PAGE NOT APPLICABLE TO US HOLDERS

NOTE: To meet local requirements, this page may be replaced when all entries are filled. The publication holder is to arrange local reproduction, and certify the replacement pages as a “true copy”. The original page numbers are to be allocated to the copy. Superseded pages should then be destroyed in accordance with applicable National instructions.

TABLE OF CONTENTS

SECTION III

DIRECTORY INFORMATION BASE

SECTION IV

COMPONENTS

SECTION V

PROTOCOLS

SECTION VI

SECURITY OF DIRECTORY

SECTION VII

MANAGEMENT OF DIRECTORY

CHAPTER 3

DIRECTORY INFORMATION

POLICIES AND PROCEDURES

SECTION I

SCHEMA DEFINITION

SECTION II

ENTRY AND ATTRIBUTE POPULATION AND USAGE

SECTION III

REGISTRATION

SECTION IV

SHADOWING

SECTION V

DIRECTORY SYSTEM PERFORMANCE

SECTION VI

CHAINING

CHAPTER 4

DIRECTORY SECURITY POLICES AND PROCEDURES

SECTION I

SECURITY

SECTION II

ACCOUNTABILITY/AUDITING

CHAPTER 5

DIRECTORY MANAGEMENT POLICIES AND PROCEDURES

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1

INTRODUCTION

101. General and Scope

a. The function of this document, Allied Communication Publication (ACP) 133, is to define the Directory services, architecture, protocols, schema, policies, and procedures to support Allied communications, including Military Message Handling System (MMHS) services based on ACP 123, in both the strategic and tactical environments. The Directory services are based on the International Telecommunication Union Telecommunication Standardization Sector (ITU-T) X.500 Series of Recommendations and the International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC) 9594. The Directory specifications will be referred to as X.500 in this document. Note that familiarity with X.500 is assumed.

b. The Allied Directory Services defined in this document are based on the 1993/1995 edition of the X.500 Directory and selected 1997 enhancements. It is expected that an evolutionary period will be necessary for existing directory services to become ACP 133-compliant. In this sense, ACP 133 is viewed as a “target”. The manner, means, and duration of such evolution are outside the scope of ACP 133.

c. This ACP applies to communication among the Allied Directory domains and within a domain for combined operations. It defines a common Directory schema which shall be supported by all Allies for international and combined operations and also records nationally unique attributes to avoid duplicate definitions of elements. It offers support for Internet mail users and transitional support for ACP 127/Joint Army, Navy, Air Force Procedure (JANAP) 128. The Directory has the potential to support different views of directory information such as white pages and yellow pages services.

d. Local interfaces and requirements, such as the specifics of terminal display and local caching, are part of this publication where required to ensure interoperability. ACP 133 includes requirements for which directory information must be displayed to the user, but the format of the display is outside the scope of this document.

e. This third version of ACP 133 defines the services, schema, and protocols required of X.500 Directory System Agents (DSAs) and Directory User Agents (DUAs) to support electronic mail (e-mail), S/MIME, Message Handling System (MHS), MMHS, ACP 127 interworking, and traditional communications. It also identifies security mechanisms that meet the security requirements for strong authentication, confidentiality, integrity, availability, and privilege/label management. As national systems and products mature, this document will be expanded to include more procedural guidance for managing the directory, support for other applications, and additional guidance for operation of tactical (mobile) directories.

102. Background

a. This ACP was written and coordinated by the Combined Communications Electronics Board (CCEB) with the Allied Message Handling (AMH) International Subject Matter Experts (ISME) working group. This group was organized to develop a common messaging strategy that can be deployed to facilitate interoperability among the Allies for military message traffic. Part of this task, and the subject of this ACP 133, was to develop a directory service that could provide access to information needed to do messaging. An ACP 133 Task Force was formed to develop Directory requirements and this ACP.

b. To ensure interoperability with North Atlantic Treaty Organization (NATO) members, ACP 133 was developed in coordination with the NATO Tri-Service Group of Communications and Electronics (TSGCE). TSGCE SC/9 is responsible for developing NATO Standardization Agreements (STANAGs) on data distribution. Rather than developing a separate NATO document, the intention is for this document to satisfy the requirements for military messaging with NATO and United Nations forces.

103. Evolution

This ACP is based on civilian international standards in order to take advantage of the availability of commercial off-the-shelf (COTS) products. As a result, the AMH ISME should monitor the future developments of the international standards and the resultant products. As new capabilities are standardized, those that are found to be useful and appropriate should be added to ACP 133. In order to maintain consistent directory service among the Allies, new versions of this ACP will be developed with formal review and coordination.

104. Overview

a. The Allied Directory is the combination of the parts of the national directories and those Combined Task Force (CTF) directories, when they exist, that are to be shared with the Allies. For example, specific unique directory requirements must be satisfied to support operations which would result from dynamic military operations. Thus, it is envisioned that the Allied Directory will consist of relatively stable shared national and combined domains, as well as, periodic dynamic combined domains to satisfy specific operations involving coalitions of national military forces and organizations, such as NATO. An overview of the Allied Directory is shown in Figure 1-1.

b. The information accessible using the Allied Directory System is contained in the Allied Directory Information Base (DIB). The information published in the Allied Directory DIB is provided to support Allied communications, including MMHS services based on ACP 123, in both the strategic and tactical environments. Besides the information used by the messaging application, the Allied Directory System supports the storage of certificates needed for secure messaging (e.g., ACP 120) and for other secure applications such as Electronic Data Interchange (EDI). The Allied Directory DIB also contains information for managing the components of the Allied communications system.

c. A Directory Management Domain (DMD) is composed of all of the directory components, policies, and information of an organization for the purposes of management. In the Allied Directory System there are two types of directory domains, as illustrated in Figure 1-1: national domains and CTF domains. The union of all national information shared is said to comprise a single logical DIB. A national domain includes the information, policy, and components needed to govern a specific nation's directory services.

d. A CTF domain is a subset of the Allied Directory that is provided by two or more Allies and includes unique mission-related information, policy, and components. The combined domain is owned, operated, and administered by a multi-national military unit. The commander of the CTF establishes the rules and procedures for its domain. No information and components are supplied or maintained by the CCEB. Rather, this ACP defines mechanisms for sharing information and interconnection of national assets to support combined operations. Note that, in this ACP, the significance of the term "combined task force" is very broad and should not be confused with specific "task force" designations already in use by various organizations such as Naval Task Force, defined by AUSCANZUKUS.

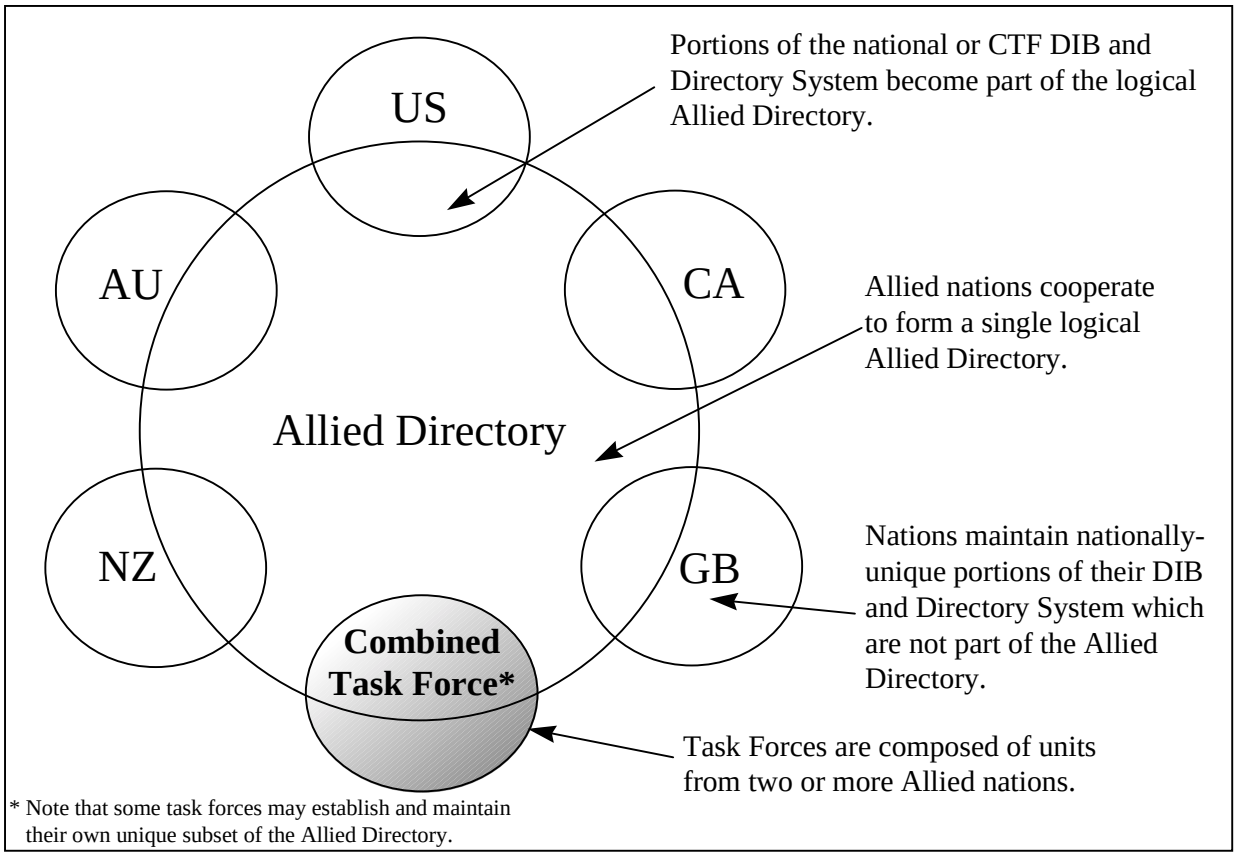

Figure 1-1
Overview of the Allied Directory

e. The X.500 Directory is composed of one or more DSAs that are the repositories for some portion of the DIB. The DIB contains user information and operational information for use by the Directory system. Each user of the Directory, whether a person or an application, uses a DUA to access the Directory. The Directory schema contains the rules governing the contents of the DIB.

f. DUAs and DSAs communicate with each other by using the Directory Access Protocol (DAP). DSAs communicate with each other using the Directory System Protocol (DSP), the Directory Information Shadowing Protocol (DISP), or the Directory Operational Binding Management Protocol (DOP). DSP is used by DSAs to "chain" requests from users when the originating or "home" DSA of the user does not have the requested information. DISP is used in the process of replicating information among DSAs. DOP is used to perform the management aspects of replication necessary for DISP and to maintain the knowledge and access control, collective attributes, and other administrative information. These components and protocols are pictured in Figure 1-2.

g. The logical arrangement of the structure of the DIB is called the Directory Information Tree (DIT). Different parts of the DIT will be managed by different organizations. To accomplish this, the DIT can be divided into subtrees called administrative areas. Policies concerning access control, schema, and collective attributes, which are explained later in this document, may then be formulated for particular subtrees.

h. The Allied Directory schema contains the rules governing the contents of the DIB. The schema includes a set of definitions for Name Forms, DIT Structure Rules, DIT Content Rules, Object Classes, Attribute Types, and Matching Rules. The Allied Directory Schema is based to the extent possible on definitions in the ITU-T X.400 and X.500 Series of Recommendations and other applicable standards for name forms, object classes, attribute types, and matching rules. Where necessary, ACP 133 defines these elements or imports definitions from other sources.

i. In addition to the user information which is controlled by the Allied Directory Schema, the Allied Directory System contains directory administrative and operational information. This system information is governed by the Allied Directory System Schema which is a set of definitions and constraints concerning the information that the Allied Directory System itself needs to know in order to operate correctly. This information is specified in terms of subentries and operational attributes. Subentries contain information relevant to a particular subtree of the DIT, and contain operational attributes. Also, user entries may contain operational attributes, such as, the last time the entry was modified.

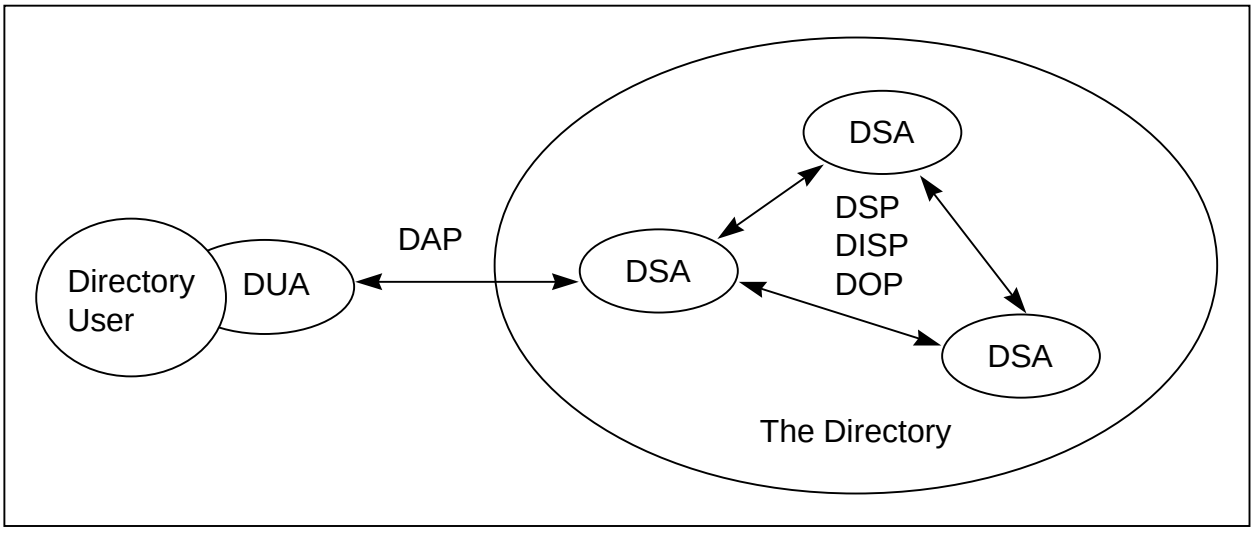

Figure 1-2
The Directory Model

105. Definitions

a. Address List - An Address List is a shorthand method for addressing a predetermined list of recipients.

b. Administrative DUA - An Administrative DUA (ADUA) is a DUA which is used by managers and administrators to query and modify user and system information in the Directory in order to manage the service and administer the information in the DIB.

c. Allied Directory Service - The Allied Directory Service is a capability provided to allied forces to support a variety of information exchange requirements. This service is implemented by the interconnection of national and CTF directory system assets which conform to this ACP.

d. Allied Directory System - The Allied Directory System consists of the components, protocols, administrators, and information that provide the Allied Directory Service.

e. Border DSA - A Border DSA is a DSA that has been designated by a DMD to provide the primary international interface for a nation's or a CTF's Directory System to the rest of the Allied Directory System.

f. Combined Task Force - A CTF is a coalition of forces contributed by two or more nations for a specific operation and period of time.

g. Common Content - The Common Content is the collection of definitions and rules about the Allied Directory System contents. It is the Allied Directory System's Directory Schema.

h. Interrogation DUA - An interrogation DUA uses the read, compare, abandon, list and search operations to query user information.

i. Interrogation/Modification DUA - An interrogation/modification DUA uses all of the Directory Services to query and modify user information.

j. National DSA - A National DSA is an "internal" DSA in a national or CTF DMD that interfaces to the Allied Directory System through a Border DSA.

k. Plain Language Address - A Plain Language Address (PLA) is an abbreviated or non-abbreviated activity (organization) title with its associated geographical location.

l. Population - Population refers to the directory entries and attributes for which values have been entered in the Allied Directory.

m. Schema Support - Support for a schema element means that it can be generated, processed, and displayed in accordance with its definition.

CHAPTER 2

SYSTEM ARCHITECTURE

SECTION I

DIRECTORY SYSTEM

201. General

The Allied Directory is a set of interconnected systems supporting subsets of the total information base. The information that is accessible by users of the Allied Directory is the same for each user, subject to access controls; that is, the Allied Directory service has the appearance of a single information base. The Allied Directory system comprises:

- the services offered to the user
- the information supplied by each Ally
- the systems in which the information is housed or used, i.e., components
- the protocols necessary for exchange of the information among the components
- the means of protecting the information and components against a variety of threats
- the means of managing the information and components.

SECTION II

USER SERVICES

202. User Access to the Directory

a. ACP 123 defines message handling services offered to the user in terms of Elements of Service (EoS) according to the definitions in the X.400 Recommendations. The X.500 Recommendations do not define services offered to the users in this way. In this document, the services that are offered to the Directory user are referred to by the term “user services”. Some user services are described as optional, that is, they are available to the user only if they are offered by the Allied Directory System. The user shall be able to select the appropriate user services for interrogation, modification, and administration of the Allied Directory.

b. Generally, the user services are employed to deal with “directory user information”, that is, the information in the directory about the entities represented by the entries. Administration is a special case of directory usage where access is also necessary to the “directory system information”, which is the information in the entries and subentries concerning the operation of the Directory itself, such as Access Control Information (ACI).

Interrogation, modification, and administration usages of the directory are illustrated in Figure 2-1. Although the figure shows human users, a directory user may be an application process, such as, an MMHS User Agent (UA).

c. The Allied Directory System provides all of the standard X.500 directory user services, which correspond to the formal operations specified for access to a directory system However, the Allied Directory System limits the use of some services by some users. For example, only authorized personnel are allowed to employ the user services that create new entries in the Allied Directory.

d. User authentication is also required by the Allied Directory Service, but in a local environment, this will be defined by national policy. Additional authentication requirements and details are addressed in paragraph 402.

e. For every user service, the results or errors from each request shall be displayed, if the user is a human.

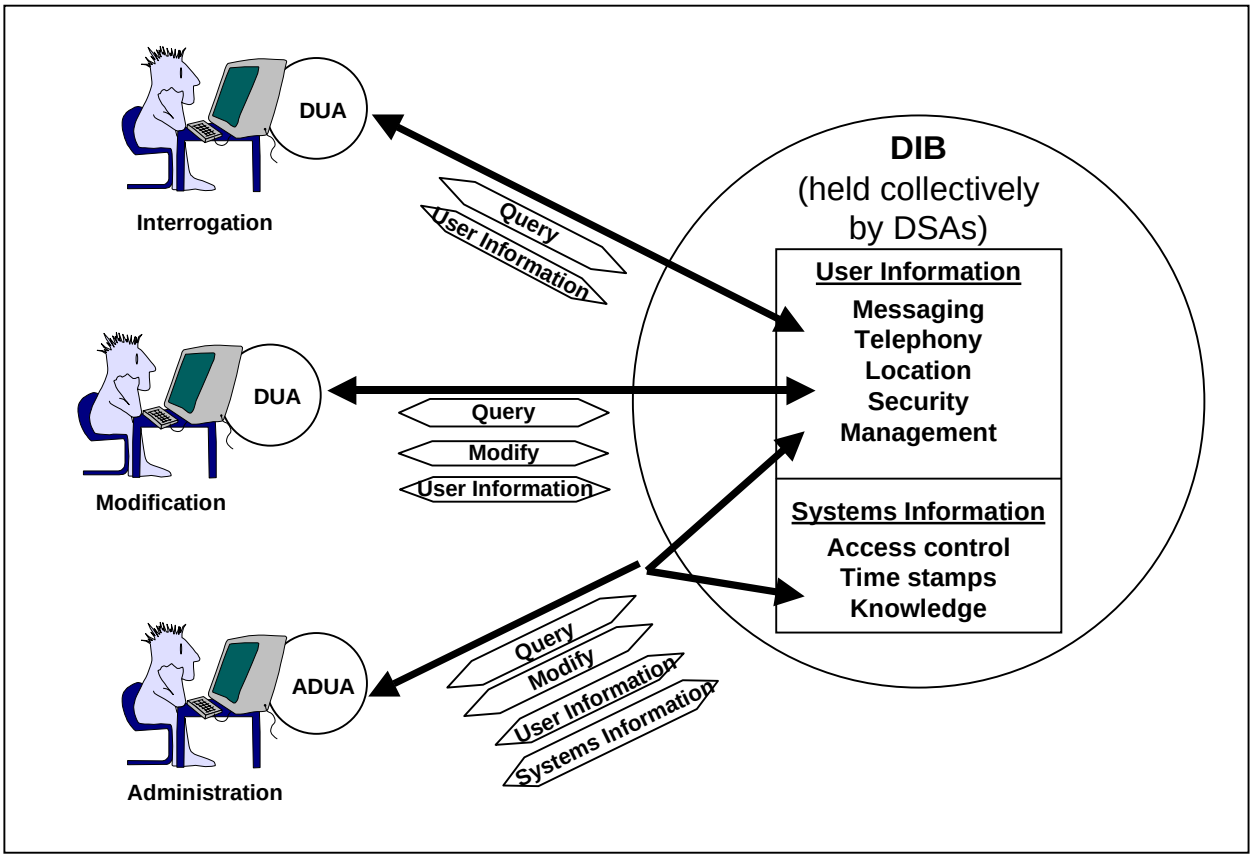

Figure 2-1
Directory User Access

203. Service Parameters and Constraints

The user services provided by the directory system can be parameterized or can be constrained by employing security parameters, by permitting filtering, and by applying entry selection criteria. In order to provide data integrity and data origin authentication, the ability to digitally sign an operation request shall be supported by the Allied Directory System. Likewise, the ability to employ the filter service constraint shall be supported.

204. Common Arguments

a. Each of the directory user services includes arguments specific to the operation being invoked. In addition, there are Common Arguments that may be used to qualify any operation, including Critical Extensions (see paragraph 205), Service Controls (see paragraph 206), and the Requestor Distinguished Name.

b. The Requestor Distinguished Name component of the common argument shall be supplied to all DSAs when records management or logging is required of DSA services or source Distinguished Name (DN) verification is performed by the DSA.

205. Critical Extensions

a. In the critical extensions component of the common argument for an operation, any enhancements that are part of the operation have the corresponding extensions listed. The requirements for the Allied Directory to support critical extensions are as follows. Also, see paragraph 219.

(1) Subentries extension shall be supported for directory administrators.

(2) Copy Shall Do extension is optional.

(3) Attribute Size Limit extension is optional.

(4) Extra Attributes extension shall be supported for Allied Directory administrators.

(5) Modify Rights Request extension shall be supported for Allied Directory administrators.

(6) Paged Results Request extension is optional. This extension shall not be used if results are to be signed.

(7) Matched Values Only extension is optional.

(8) Extended Filter extension is optional.

(9) Target System extension is optional.

(10)Use Alias On Update extension shall be supported for those Allied Directory users that require directory modification user services.

(11)New Superior extension shall be supported for Allied Directory administrators.

b. The following extensions specified in X.511 ’97 edition shall be supported for Allied Directory administrators:

(1) For DAP, DSP, and DISP, signed response for those operations which in X.500 ’97 returned a Null result (e.g., DAP operations Add Entry, Remove Entry, Modify Entry, Modify DN and all DISP operations)

(2) Signed errors

(3) The extensions for security parameters:

- operationCode
  (Note: a defect in the syntax for operation code is being reported.)

- errorCode
  (Note: errorCode is added to security parameters in a defect being reported.)

- procedures for setting the random value in operation result/error

206. Service Controls

a. The Service Controls component of the Common Arguments contains controls that direct or constrain the provision of the directory user services. For example, the priority of the request can be set, or time and/or size limits can be set on the operation responses. Allied Directory support for Service Controls is as follows.

(1) PreferChaining is optional.

(2) ChainingProhibited is optional.

(3) LocalScope is optional.

(4) DontUseCopy is optional.

(5) DontDereference Aliases shall be supported.

(6) Subentries shall be supported for Allied Directory administrators and is optional for other Allied Directory users.

(7) CopyShallDo is optional.

(8) Priority shall be supported. In an ACP 123 environment, this service control shall follow the Grade of Delivery EoS for which the messaging request is made. That is, for directory operation requests that are part of processing a message, the Messaging Grade of Delivery EoS Non-urgent should map to the Directory low priority, Normal should map to medium, and Urgent should map to high. Note that this is not a guaranteed service in that the Directory as a whole,

does not implement priority queuing. There is no relationship implied with the use of priorities in underlying layers.

(9) Time Limit is optional. It shall be monitored by the DSA and have configurable pre-set values to ensure the Allied Directory System is not compromised. Since this service control is dependent on a number of factors, including synchronization between DSA clocks, it is recommended that the abandon user service be used to abort operations which are not completed in the required period of time.

(10)Size Limit is optional. It shall be monitored by the DSA and have configurable pre-set values to ensure the Allied Directory System is not compromised.

(11)Scope Of Referral is optional. It shall be monitored by the DSA and have configurable pre-set values to ensure the Allied Directory System is not compromised.

(12)Attribute Size Limit is optional. Its use is a national matter.

b. Certain combinations of Priority, Time Limit, and Size Limit may result in conflicts. For example, a short time limit could conflict with low priority; a high size limit could conflict with a low time limit, etc.

c. The Service Controls component of Common Arguments shall be supported as an essential feature in all Allied Directory DSAs and DUAs. However, its use is mainly associated with distributed directories, directory management, or controlling response requirements.

207. Distributed Directory Service

Many of the service control facilities deal with parts of the distributed directory information model, e.g., DMD definitions, referrals, master/copy entries. These aspects of distributed directories are subject to national and allied operational requirements.

a. Distributed operations control may employ the following service control elements: Prefer Chaining, Chaining Prohibited, Local Scope, and Scope Of Referral.

b. Master/copy entry selection may employ the following service control elements: Dont Use Copy and Copy Shall Do. Their settings will depend on the user requirement to retrieve master or copy information.

c. Request/response characteristics may be controlled using the following service control elements: Priority, Time Limit, Size Limit, and Attribute Size Limit. In the Allied Directory System, these facilities shall be configurable in ADUAs. For other DUAs, priority should default to medium. The default for Time Limit should be 60 seconds. The default for Size Limit should be set to the number of objects that can be contained in 250 kilobytes. (This can be adjusted for the Directory application and nature of the DUA-DSA access link.)

208. Common Results

The Common Results shall be supported. However, its use should be defined with respect to the application's needs.

SECTION III

DIRECTORY INFORMATION BASE

209. Allied Directory Schema

The Allied Directory Schema encompasses the directory entry types, object classes, attributes, matching rules, name forms, and structure rules that are necessary for specifying the information that is stored in the Allied Directory System. Components of the Allied Directory System shall implement all of the standard object classes, attributes, and name forms defined in X.501, X.509, X.520, X.521, and X.402, as profiled in Annex D. The Allied Directory Schema, called Common Content, employs the standard schema elements and also includes object classes, attributes, and name forms defined in this ACP especially to meet Allied requirements. The Allied Directory Schema is specified in Annex B and is profiled in Annex D.

210. Directory Entries for Messaging Users

One purpose of the Allied Directory is to provide access to stored information about organizations and individuals in various Allied domains to enable them to exchange messages, that is, to be users of the message exchange services defined in ACP 123. The stored information is the DIB in which each entry represents a user or group of users. Three types of entries are defined, corresponding to the organizational unit, organizational role, and organizational person (individual) categories of messaging users. A fourth type of entry, address list, is defined for representing groups of users.

211. Content Rules

a. Content rules are used for two purposes in defining Allied Directory entry types.

b. First, a content rule can be used to define one or more entry types with a base structural object class by adding auxiliary object classes and adding (or deleting) attributes without creating a new object class. For example, an MHS Message Store (MS) entry may be defined by specifying the mhs-message-store structural object class, the securePkiUser auxiliary object class, and aliasPointer, effectiveDate, and expirationDate optional attributes in an aCPMhs-message-storeRule content rule. The auxiliary object classes listed in a content rule are not required to be used in every instance of the type of entry specified. Each allowed auxiliary object class that is used in an entry is identified in the value of the entry's objectClass attribute. For example, using the aCPOrganizationalPersonEdBRule content rule defined in Annex B, an entry for every instance of Organizational Person would have to include commonName and surname. If the person does X.400 mail, the object identifier for mhs-user would be added to the

entry, and this would make mhs-or-addresses mandatory and mhs-deliverable-content-types optional. If the person needs a certificate, the object identifier for securePkiUser would be added to the entry, and userCertificate would be allowed. The end result is that the Directory could contain entries for different persons with different mandated attributes. The use of a content rule to define one or more entry types is used extensively in defining the Common Content.

c. Secondly, the directory standard requires the use of a content rule to allow the application of collective attributes to an entry type, since none of the object classes are allowed to contain collective attributes. For example, ACP 133 uses the standard object class for organizational person, in which postal address is an attribute. The local administrator may choose to make the postal address a collective attribute, if that is more efficient than entering a postal address in the entry for every individual at the same location. In this case, a content rule permitting the collective postal attribute would have to be defined and applied. The example content rules given in Annex B would require modification to permit collective attributes in entries.

d. Nations may add nationally-specific attributes to the example rules, given in Annex B; however, this may affect management and interoperability of the directory information in combined environments.

212. Directory Information Tree

Entries in the Allied Directory are arranged in the form of an inverted tree, called the DIT, where the vertices represent the entries. Each entry adds the value of one or more attributes. The ordered list of the values of the branches through the tree to a user entry is the DN for the entry. The entries highest in the Allied Directory tree represent countries and international/multinational organizations (such as NATO), those in the middle represent organizations and localities, and those at the bottom represent individuals, application processes, address lists, etc.

213. Subtrees

a. The Allied Directory DIT is specified by this ACP, with some levels defined by national policy as shown in Figure 2-2 and described here. For each Ally, Country is the initial entry under the root. The definition of the Country entry and the location of the master entry for Country are controlled by the country itself and are outside the scope of this ACP. The Country entry described in Annex B assumes the standard definition from X.521, which is satisfactory for purposes of the Allied Directory. The arrangement of the ally-specified levels of the DIT, the values of the entries, and the location of the master entries are a matter of national policy and are outside the scope of this ACP. However, each of the Allies has provided this information for inclusion in Annex B. Although published here, this ACP is not the official source for this national information.

b. Below the Country entry of an Ally, one of the subtrees includes the armed forces of the Ally, e.g., Department of Defense for the U.S. The armed forces are represented by an

organization or organizational unit. Below the armed forces level each Ally has defined the subtrees that contain the information needed to represent its forces, including Services, agencies, and commands. The commands include the CTFs that are led by the Ally. The armed forces subtrees of each Ally are shown in Annex B.

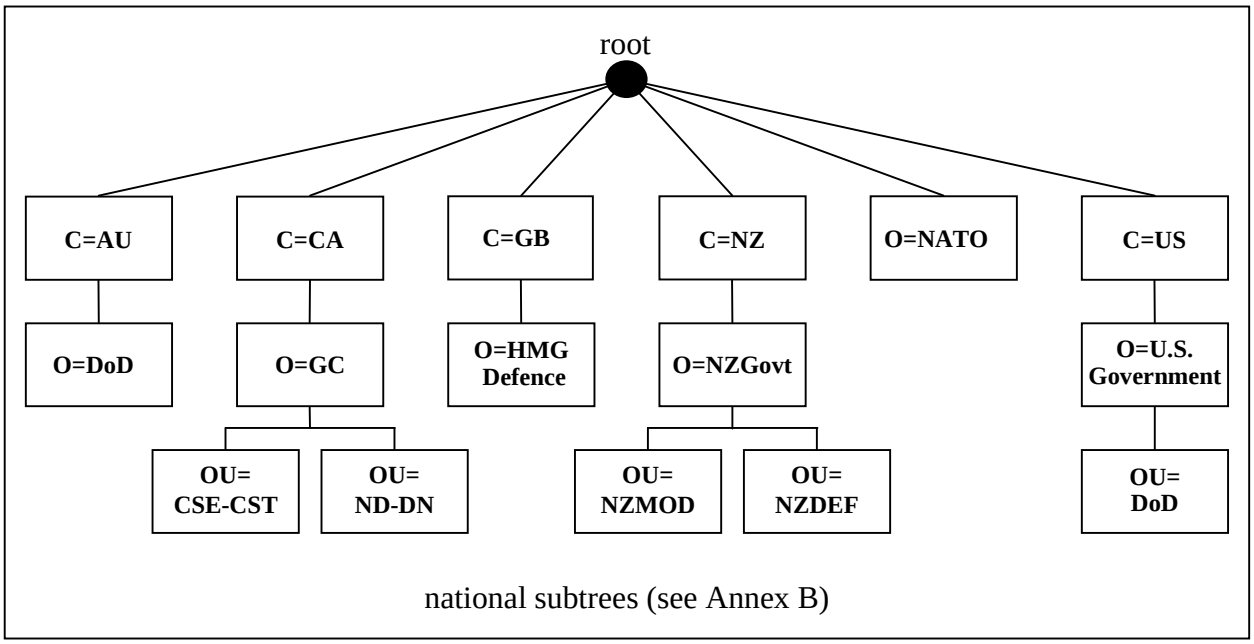

Figure 2-2
Top-Level Allied Directory DIT

SECTION IV

COMPONENTS

214. General

a. The components of the Allied Directory System are: DSAs, Border DSAs, and DUAs. An example of interconnecting these components is illustrated in Figure 2-3.

b. This section applies to both national and combined domains described in paragraph 104. The DSAs within a CTF domain are termed “National” and “Border” in a manner analogous to a national domain. That is, a National DSA in a CTF domain is only connected to DSAs within the domain and connections to other domains are made by Border DSAs.

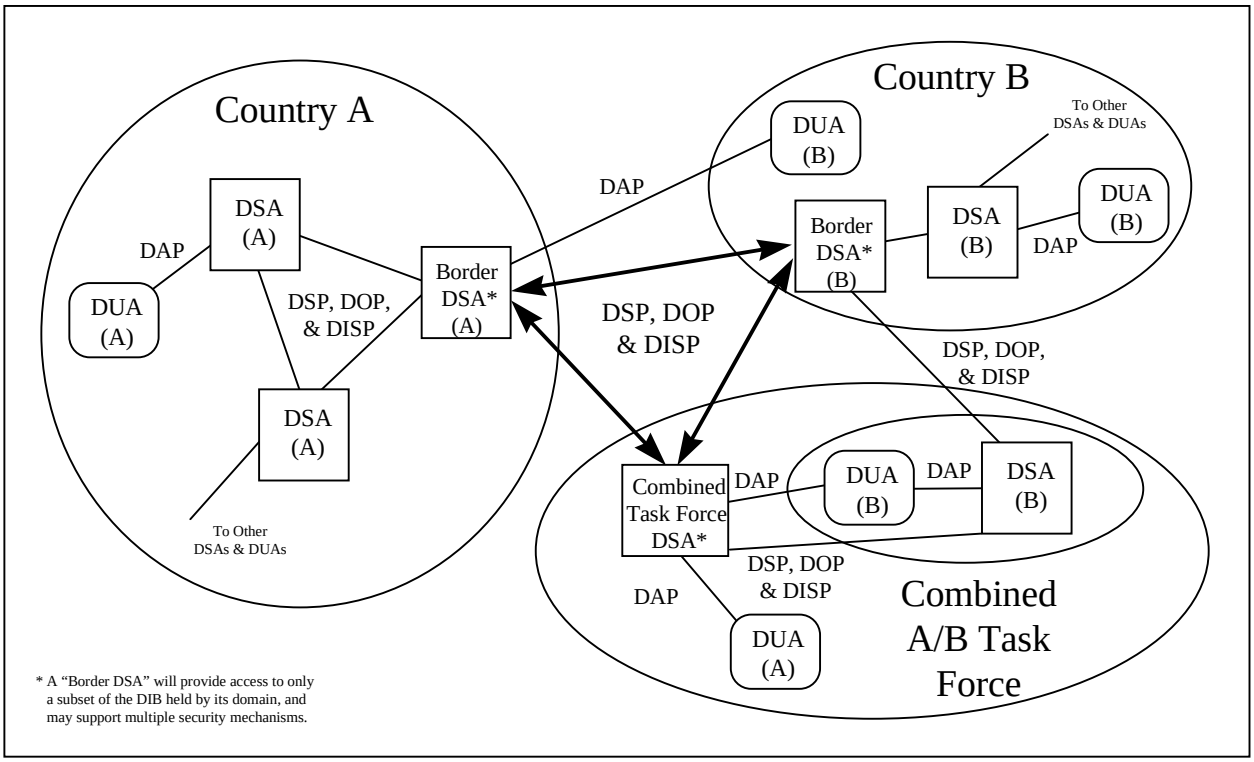

Figure 2-3
Example Allied Directory Configuration

215. DSAs

a. DSAs, collectively, hold the Allied DIB and interact with one another to make the entire DIB accessible to the directory users. The directory system is comprised of DSAs that interact with one another to perform the directory services described above. The DSAs interact with DUAs to get user requests and provide the results from processing the requests.

b. Within each DMD, the distribution of directory information among multiple DSAs is a national/combined task force matter, subject to the quality of service, management, and security provisions of this ACP.

c. The Allied Directory System is composed of a two-tier hierarchy of DSAs: Border DSAs and National DSAs. Both types of DSAs provide functionality as specified in International Standardized Profiles (ISP) 1993 Directory Application Profile (ADY)21, ADY22, ADY42, ADY43, ADY45, 1993 Directory Interchange Format and Representation Profile (FDY)11, and FDY12 with the further requirements defined in Annex D.

d. The contents of National DSAs are a national matter, except that a common definition of National DSA contents is necessary for interoperability of assets from different nations in CTF domains. Note that the contents of the Border DSAs and National DSAs are the information the

ally makes available in the Allied Directory System. Which Services/agencies/commands, entries, or attributes from the national directory service are included in the Allied Directory System is a national or CTF matter. A combination of Directory access controls (and other separation mechanisms) may be used to effect the segregation of domain-specific and shared information.

e. The time limit argument of Chaining Arguments is dependent on synchronization between DSA clocks to an order of magnitude less than the time limit. If such synchronization cannot be achieved, it is recommended that the chained abandon service be used to abort operations which are not completed in the required period of time.

216. Border DSAs

a. A Border DSA is a logical DSA that has been designated to provide the primary international interface for a nation's or CTF's directory system. The implementation of an instance of a Border DSA may be a specific or separate component or a logical partition of the information. Border DSAs are interconnected to enable the sharing of directory information across DMDs. Within a CTF, DSAs from the participating Allies shall interoperate in accordance with this ACP.

b. A Border DSA shall perform many functions that ordinary DSAs within a nation or CTF need not support. One of the major functions of a Border DSA is to provide the portion of the national/task force DIB available for access in the Allied Directory System. Thus, some portions of the national DIB may be unavailable. Also, a different security policy may apply to Border DSAs than national DSAs.

c. The process for resolving directory queries within a particular national directory domain is beyond the scope of ACP 133. Valid options include utilizing a shadow of the national/task force DIB maintained locally within the Border DSA, chaining the query onward into the national/task force domain, or providing a referral to a specific internal DSA that can be accessed by the user. A nation/task force may designate any number of DSAs as Border DSAs.

217. DUAs

a. The directory access facilities required by the Allies dictate that DUA functionality is provided in a number of forms. DUA functionality will be embedded into commercial products which provide the user desktop services as well as providing specific infrastructure functions such as information retrieval for Message Transfer Agents (MTAs).

b. DUAs make requests on behalf of the directory user and present results back to the user. For example, a user can request the Originator/Recipient (O/R) address of a messaging user in another country. DUAs are interconnected with DSAs (including Border DSAs). DUAs provide functionality as specified in ISPs ADY11, ADY12, ADY41, FDY11, and FDY12 with the further requirements defined in Annex D.

c. The degree to which a DUA is integrated with a UA, e.g., a Military Messaging User Agent (MMUA) or Mail List Agent (MLA) or other application that is a directory user, varies

according to the application, its implementation, and the degree of human involvement in directory information access. A DUA may be an entirely independent application.

d. ACP 133 defines three types of DUA functionality. DUAs with different functionality than is defined here may be used as a national option.

(1) An "Interrogation" DUA uses the Read, Compare, List, Search and Abandon services only. This type of DUA enables directory users to request information from entries. These services may be constrained by the limitations of the DUA, and they are limited by the DSA access controls.

(2) An "Interrogation/Modification" DUA uses all of the Directory services. Such a DUA enables directory users to obtain information by directly reading an entry or by locating interesting entries based on their content or partial name as well as modify entries. These services may be constrained by the limitations of the DUA, and they are limited by the DSA access controls.

(3) An "Administrative" DUA uses all of the Directory services. This type of DUA enables a directory user to act as a Directory System Administrator, creating, modifying, and deleting user entries and directory operational information. Access controls will limit what functions of an Administrative DUA may be used by a specific user.

e. Authentication of DUAs is addressed in paragraph 402.

f. A DUA may receive a continuation reference when a DSA responds to an operation by issuing a referral to another DSA. A DUA might also receive a continuation reference as part of an incomplete List or Search result.

(1) Some DUAs may be designed for use in environments where such references are never used, or a DUA may be simplified such that it cannot pursue a reference. Alternatively, a DUA may be designed to be capable of pursuing references. Another possibility is that a DUA product is designed to be configurable such that the capability to pursue references may be controlled (either by the user or by the system administrator). In any case, when a DUA does not automatically pursue a continuation reference, the reference shall be passed to the user so that a procedure can be used instead.

(2) Continuation references received in List or Search operations shall be handled by the receiving DUA (by displaying them, etc.); however, their automatic continuance by the DUA will be subject to national policy. In general, so that search or list loops are deleted, it is preferable that continuation references be performed by DSAs rather than by DUAs.

SECTION V

PROTOCOLS

218. General

a. To ensure interoperability among DUAs and DSAs from different nations, the X.500 standard protocols are used for Allied Directory communications. These protocols are:

- DAP
- DSP
- DISP
- DOP

b. Figure 2-3 shows which protocols apply to each type of interconnection. Use of these protocols is a requirement within a CTF domain. Otherwise, use of these protocols within a national domain is outside the scope of this ACP.

219. DAP

a. DAP is used to convey requests for directory information to a DSA and to return the results to the DUA. DAP is used between a DUA and a Border DSA in different domains and between a DUA and a DSA in a CTF domain. DAP shall be implemented as specified in ISPs ADY11, ADY12, ADY21, ADY41, and ADY42 with the further requirements defined in Annex D.

b. DAP is used to access the Services of the Allied Directory.

(1) Table 2-1 shows the DAP operations that shall be implemented by each type of DUA.

Table 2-1
DAP Operations Implementation

Operation	Interrogation DUA	Interrogation/ Modification DUA	Administrative DUA
bind	m	m	m
unbind	m	m	m
read	m	m	m
compare	m	m	m
abandon	m	m	m
list	m	m	m
search	m	m	m
add entry	o	m	m
remove entry	o	m	m
modify entry	o	m	m
modify DN	o	m	m

(2) DSAs shall implement all DAP operations.

(3) Table 2-2 shows support for Critical Extensions.

Table 2-2
1993 Critical Extensions Support Summary

Extension	Interrogation DUA	Interrogation/ Modification DUA	Administrative DUA	DSA
subentries	o	o	m	m
copyShallDo	o	o	o	m
attributeSizeLimit	o	o	o	o
extraAttributes	o	o	m	m
modifyRightsRequest	o	o	m	m
pagedResultsRequest	o	o	o	o
matchValuesOnly	o	o	o	o
extendedFilter	o	o	o	o
targetSystem	o	o	o	o
useAliasOnUpdate	o	m	m	m
newSuperior	o	o	m	m

Table 2-3
1997 Extensions Support Summary
(see X.511(1997) §7.3.1 Table 1)

Extension	Interrogation DUA	Interrogation/ Modification DUA	Administrative DUA	DSA
manageDSAIT	o	o	o	o
useContexts	o	o	o	o
overspecFilter	o	o	o	o
selectionOnModify	o	o	o	o
Security parameters - response	o	o	o	o
Security parameters - operation code	o	o	m	m
Security parameters - attribute certification path	o	o	o	o
Security parameters - error protection	o	o	o	o
Security parameters - error code	o	o	m	m
SPKM Credentials	o	o	o	o
Bind token - response	o	o	o	o
Bind token - Bind Int. Alg, Bind Int Key, Conf Alg and Conf Key Info	o	o	o	o
Bind token - DIRQOP	o	o	o	o

220. DSP

a. DSP is used to convey an information request to another DSA when the requesting DSA does not have the complete information requested, i.e., to do chaining, and to return the results to the requesting DSA. DSP is used between Border DSAs in different domains and between a DSA/Border DSA and another DSA in a CTF domain. DSP shall be implemented as specified in ISPs ADY22, ADY43, ADY45, and ADY61 with the further requirements defined in Annex D.

b. DSP consists of the operations, results, and errors defined for DAP plus additional information exchanged among the DSAs to notify each other of the progress and results of the operation.

(1) The operations defined in DSP are:

- bind
- unbind
- chained read
- chained compare
- chained abandon
- chained list
- chained search
- chained add entry
- chained remove entry
- chained modify entry
- chained modify DN

(2) Any of the DSP operations can be initiated by any DSA. In particular, the DSA that receives a request from a DUA is responsible for initiating the first chaining operations, when necessary. Then, if further chaining operations are needed, whichever DSA needs more information initiates the next operation.

c. When requested information is not present in the home DSA, chaining is preferred over referral for access to international information. To access information that is specific to country B, a DUA within country A would access the directory through its home DSA. The home DSA would chain the operation to the appropriate Border DSA within country A. Depending on the specific information requested and on the shadowing agreements that are in place, the country A Border DSA may either complete the operation locally or further chain the operation to a country B Border DSA. Similarly, the Border DSA in country B may contain a master or shadow copy of the desired information, or it may chain the request onward within country B. Both chaining and referrals shall be supported in the Allied Directory (see paragraph 323).

d. DSAs shall support in DSP the same critical extensions supported for DAP as shown in Table 2-2.

221. DISP

a. DISP is used to replicate information in the Allied Directory by conveying shadow copies of directory information from one DSA to another as described in paragraph 316. DISP is

used between Border DSAs in different domains and between a DSA/Border DSA and another DSA in a CTF domain. Prior to using DISP, an agreement to shadow is arranged and activated. In the DSA sending the shadow, the information may be the master copy or a shadow copy of the information. Both primary and secondary shadowing shall be supported. DISP shall be implemented as specified in ISPs ADY51, and ADY62 with the further requirements defined in Annex D.

b. The operations defined for performing the replication of the Directory Information are:

- bind
- unbind
- request shadow update
- update shadow
- coordinate shadow update

c. All DSAs that implement shadowing shall implement all of the DISP operations.

d. Which DSA initiates each of the DISP operations depends on which DSA is the consumer and supplier, as arranged in the shadowing agreement.

222. DOP

a. DOP is used to activate, deactivate, and modify shadowing agreements that have been arranged between DSAs and to exchange knowledge and access control, collective attributes, and other administrative information contained in subentries. DOP is used between Border DSAs in different domains and between a DSA/Border DSA and another DSA in a CTF domain. DOP shall be implemented as specified in ISPs ADY71 and ADY72 with the further requirements defined in Annex D.

b. The operations defined for DOP are:

- bind
- unbind
- establish operational binding
- modify operational binding
- terminate operational binding

c. All DSAs that implement shadowing or exchanging knowledge or other administrative information shall implement all of the DOP operations.

d. The DSA that initiates the association is the initiator of the DOP operations performed in the association.

223. Underlying Protocols

All of the Directory protocols include the Association Control Service Element (ACSE) and operate over the Presentation and Session Layer protocols. These protocols are profiled in ISO/IEC ISP 15125-0, Common Upper Layer Requirements (CULR) for the Directory. Below the Session Layer, the directory applications require a connection-oriented transport service that may be provided in a variety of ways, depending on the underlying networks and internetworking environment.

SECTION VI

SECURITY OF DIRECTORY

224. Security Mechanisms

The Directory protocols include security mechanisms that meet the security requirements for the Allied Directory System. Therefore, no additional protocols are employed to protect the Allied Directory System and Services.

SECTION VII

MANAGEMENT OF DIRECTORY

225. Management Architecture

a. Figure 2-4 illustrates a model for systems management interfaces for the Directory. The interfaces that do not indicate a protocol, such as, between a DSA and a management agent, are not standardized.

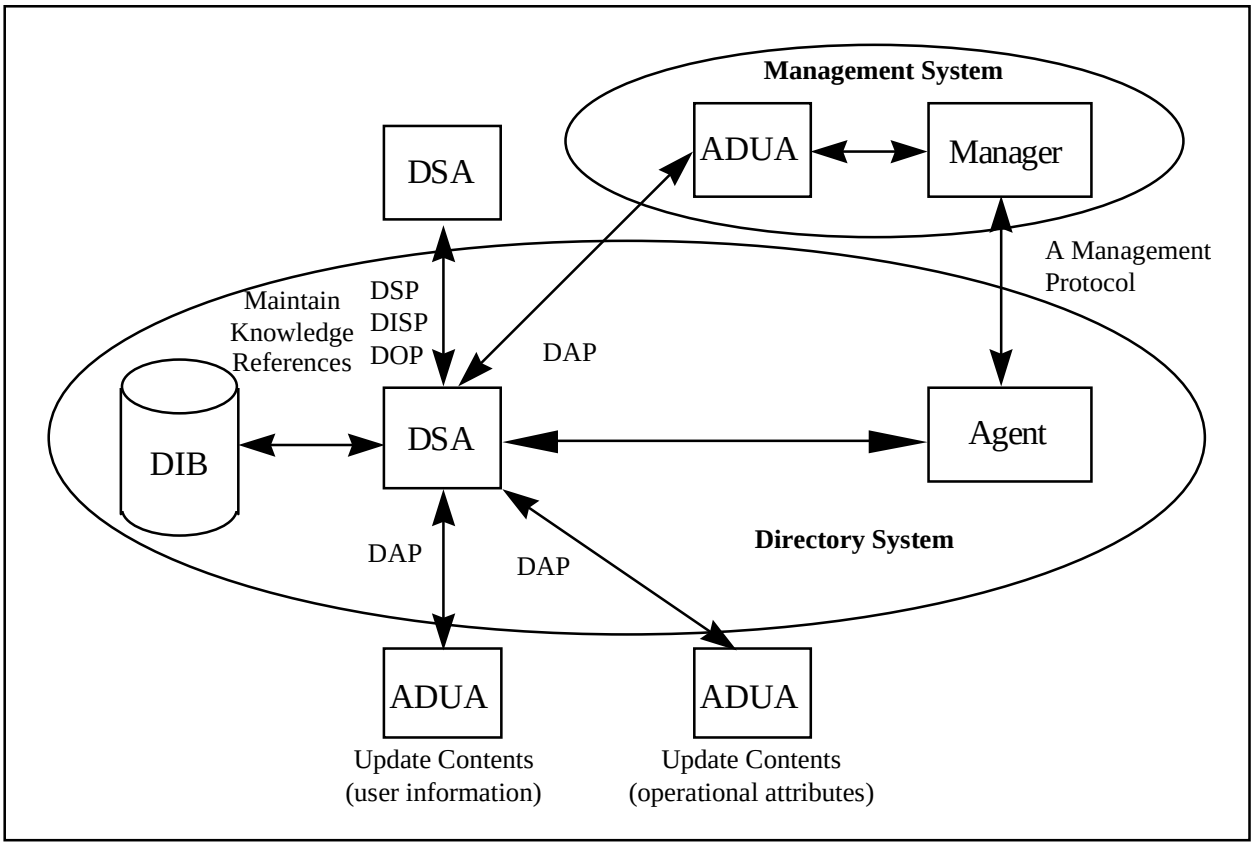

Figure 2-4
Model for Management of the Directory

b. All aspects of management leading to processing, recording, communication and logging of information shall be configurable.

226. Management Protocols

Management protocols, such as Common Management Information Protocol (CMIP) or Simple Network Management Protocol (SNMP), are outside the scope of this ACP.

227. Year 2000 and Date/Time Format

a. Background

(1) The format for date/time in X.500 in some instances is defined as UTCTime. This format is not Y2K compliant because it uses two digits to represent the year. New definitions use GeneralizedTime, which uses four digits to represent the year.

(2) Some of the problems with UTCTime have been corrected by technical corrigenda (TC). TC2 to X.520 amended the UTC Time Match to say that “UTC times with year values 50

to 99 shall be taken to represent times that are earlier than UTC times with year values 00 to 49." TC3 to X.509 replaced UTCTime with Time, which is a choice of UTCTime or GeneralizedTime and gave directions on how to rationalize UTCTime into a four-digit year value.

(3) Both of these corrigenda have been included in the 1997 edition of the Directory specifications, and they are referenced in the latest drafts of the ISPs for the 1993 edition of X.500. A draft TC is being processed to add the choice of UTCTime to the other occurrences of time in X.500. The reason that a choice was added rather than changing occurrences of UTCTime to GeneralizedTime was for backward compatibility. Eventually the use of UTCTime should be phased out.

b. UTCTime

(1) UTCTime values shall be expressed as Greenwich Mean Time (Zulu) and shall include seconds (i.e., times are YYMMDDHHMMSSZ), even where the number of seconds is zero.

(2) To correctly interpret UTCTime past the year 2000 (Y2K) the two-digit year associated with UTCTime shall be rationalized into a four-digit year value as follows:

(3) if the 2 digit value is 00 through 49 inclusive, the value shall have 2000 added to it;

(4) if the 2 digit value is 50 through 99 inclusive, the value shall have 1900 added to it.

(5) In no case shall UTCTime be used for representing dates beyond 2049. Definitions of new schema elements that include time are to be defined as specified in paragraph 302.

c. GeneralizedTime

GeneralizedTime values shall be expressed as Greenwich Mean Time (Zulu) and shall include seconds (i.e., times are YYYYMMDDHHMMSSZ), even where the number of seconds is zero. GeneralizedTime values shall not include fractional seconds.

d. Interworking

The use of GeneralizedTime may prevent interworking with implementations unaware of the possibility of choosing either UTCTime or GeneralizedTime. It is the responsibility of those specifying the ACP 133 domains in which allied systems are interconnected that this specification be used.

e. Certificate Validity

The certificate validity period is the time interval during which the CA warrants that it will maintain information about the status of the certificate. The field is represented as a

sequence of two dates as defined above: the date on which the certificate validity period begins (notBefore) and the date on which the certificate validity period ends (notAfter). Both notBefore and notAfter may be encoded as UTCTime or GeneralizedTime.

f. Audit Trails and Engineering Logs

Although it is unlikely that audit trail information and engineering log information from ACP 133 (interworking) systems will be exchanged between allies. It is requested that all the support and management facilities of ACP 133 compliant systems are Y2K compliant. Each nation should request such compliance for these management areas when selecting their products/vendors.

CHAPTER 3

DIRECTORY INFORMATION

POLICIES AND PROCEDURES

SECTION I

SCHEMA DEFINITION

301. Schema

The schema policy for ACP 133 is to support the Allied Directory schema and the Allied Directory system schema as profiled in Annex D using the schema specifications given in Annex B. The Allied Directory schema, which is called the Common Content, includes the specification of user information stored in the Directory. The Directory system schema includes the specification of information that is required to control and manage the DSAs themselves. Support for a schema means that a DUA or DSA shall be able to handle the information types (e.g., object classes, attribute types).

a. Common Content

(1) The Common Content includes object classes, name forms, matching rules, and attributes from the X.500 and X.400 standards, from Request for Comments (RFC) 1274, and those defined in this ACP. The Common Content is summarized in Table B-55. The types of attributes that are present in a directory entry is dependent on the object class or classes to which the entry belongs. ACP 133 specifies the attributes and object classes in the Common Content that must be supported for military applications.

(2) Requirements and guidelines for population of the Common Content for specific applications are found in paragraph 311. A few supplementary attributes, which are not defined as a part of the Common Content, but may be used by two or more nations, are included in Annex B. These are termed “useful attributes”. Useful attributes shall not be replicated, unless specific bi-lateral arrangements are made for their support on both the supplier and consumer systems.

(3) Nations may need to define additional objects and attributes. The schema for the Allied Directory does not preclude such extensions. However, the additional information stored in national extensions might not be accessible as part of Allied Directory Services.

(4) For the interoperation of ACP 127/JANAP 128 systems and ACP 123 systems, provision is made in the Common Content for including information about PLAs.

(5) The Allied Directory System shall enforce the Common Content to ensure that the structure and contents of the DIB remain well-formed over time as modifications are made. Action is taken to prevent the wrong attributes being added for an object, to ensure that the

values are in the correct form for the attribute type, and to ensure that objects are correctly placed in the DIT.

b. Directory System Information

The system schema for the Allied Directory System includes operational attributes such as the time an entry was created, knowledge references, designation of administration points, and ACI. The system schema supported by the Allies is specified in Annex B and profiled in Annex D. The meaning of support for system schema elements is explained in FDY12.

c. Support by DUAs and DSAs

(1) All DSAs and DUAs, including ADUAs, shall support the Common Content in accordance with Annex D. DSAs and ADUAs shall also support the system schema in accordance with Annex D.

(2) Use of MLAs is a national/CTF matter.

(3) Use of MHS distribution lists is a national/CTF matter.

(4) Use of alias pointers is a national/CTF matter.

(5) The application of collective attributes to the DIT is subject to national/CTF policy.

d. Management Information

The Allied Directory System may contain a range of information objects for the purpose of supporting the management of the communications system. This management information is in addition to the management information that supports the management of the directory system itself such as operational attributes, subentries, and knowledge references. These additional management objects provide support for message routing, system functions (such as MTAs and gateways), communications profiles, and logging entities, etc. These objects, where possible, use definitions as specified in the relevant standard (e.g., ISO/IEC 10021-10 and RFCs 1801, 1836, 1837 for X.400 routing and management). Currently, none of these standards is covered by the Common Content.

302. Time Definitions

All new definitions related to time shall use the data type Generalized Time. (Generalized Time uses a four-digit representation of the year of Universal Coordinated Time (UTC) rather than a two-digit representation.)

303. Directory Names

a. Each nation or international organization is responsible for assuring the uniqueness of names in its subtree.

b. The DIT should be organized to keep the number of levels as few as possible and to have no more than ten levels.

c. An individual may have multiple identities. For example, one person may have one identity as an individual and another as a security officer or other role. The person's name would be included in the entry for the role as role occupant. Alternatively, many individuals may support a single role function. The commonName would reflect the role name convention. The seeAlso attribute may be used to cross-reference the entries holding the other identities.

d. Additional values besides the distinguished value may be included in naming attributes. An additional name allows for different values to produce a successful result when searching for an item in the Directory. For example, the commonName attribute could include the Relative Distinguished Name (RDN) value: “Smith, Robert K” plus an additional name: “Bob Smith”.

e. Each entry in the Allied Directory has a unique and globally unambiguous name, the DN, which is composed of the values of the attributes indicated for naming in the DIT. For example, a person’s name could be { C=US, O=U.S. Government, OU=DoD, OU=Navy, OU=locations, L=Washington DC, CN=Jackson, Robert }.

f. The values of attributes composing directory names (i.e., DNs) should be kept as short as possible while remaining meaningful and unique.

g. In order to avoid reassigning users' directory names each time they are promoted, a rank indication shall not be included in the common name distinguished value of the relative RDN attributes of persons. The rank attribute is used for this purpose.

h. When creating a directory name, any appropriate combination of upper and lower case characters may be used in character string values, as directory operations are case insensitive in matching character strings for selecting an entry.

i. For naming an organizational person, this ACP permits the RDN to have multiple components, that is, have a distinguished value in more than one attribute. For example, the RDN could be a distinguished value of commonName plus a distinguished value of organizationalUnitName.

j. Using a DN qualifier as a second component of an RDN to identify an entity in the directory uniquely is permitted for some types of directory entries. For example, the RDN of an Organization entry could be a distinguished value of organizationName plus a distinguished value of dnQualifier.

(1) In order to ensure that these qualifiers are used in an optimal way, the following naming policy is recommended.

(a) Where possible, the RDN should consist of a single component.

(b) Since conflict may arise with some object names, provision is made for the DN Qualifier to be used in addition to the mandatory naming attributes for Organizational Person Ed. A, Organization, Organizational Role Ed. A, Organizational Unit Ed. A, Application Entity Ed. A, Certification Authority Ed. B, Release Authority Person Ed. A and Role Ed. B entries. This DN Qualifier must be locally administered.

(c) In the directory systems that support Certificate Management Infrastructure (CMI) applications, it may be desirable to organize the CA's certificate and user's certificate release information that have common properties into "domains".

(2) This directory organization optimizes the certificate path processing and CA operational management. When organized in such a fashion, CA directory entries require a multi-component RDN. ACP 133 satisfies this requirement by permitting DN Qualifiers in the name forms for organization, organizational unit, organizational role, and application entity object classes.

(3) The use of DN Qualifier in ACP 133 has the semantics of a unique identifier and not the precise meaning as defined in X.520.

k. Although the localityName and stateOrProvinceName attributes are optional in the locality object class in X.521, one or the other of them shall be present in Locality entries in the Allied Directory because they are the naming attributes for localities.

l. The RDN shall not include the full stop character (period), even when an abbreviation is included in the value.

m. The distinguished value of common name of an organizational person shall be in the order: last name, first name, middle initial (s), generation qualifier. Other values of common name may be ordered differently.

n. A directory object may have one or more alias entries that point to the object entry. For example, an EDI party name may be an alias that maps to the Directory name of an organization. Another example is the temporary maintenance of an alias for an individual at one location when he has been transferred to another location.

o. When aliases are used, there is a need to keep them synchronized with the DNs they point to. Standardized management tools will be needed to perform this alias/distinguished name synchronization.

304. Organizational Roles

Provision is made in Common Content for nations to establish directory entries for functional roles in addition to entries for individuals and organizations. These entries will tend to be more stable than those for individuals and may be especially useful for tactical organizations. In addition to a generic organizational role, three roles are recognized in this ACP: Certification Authority (CA), Security Officer, and Release Authority.

305. Certification Authority Function

In the Allied Directory, the CA function may be represented as a special case of an organizational role object. Alternatively, a CA can be represented in the Allied Directory as a special case of any of three other objects: organization, organizational unit, or application entity. In any case, the distinguished value of the commonName, organizationName, or organizationalUnitName attribute of a Certification Authority Ed. B directory entry is a national issue. The naming conventions associated with each nation's CA will be in accordance with each nation's Certificate Policy and Certification Practice Statement (CPS).

306. Security Officer Function

The role of security officer for an organization is represented in the Allied Directory by an Organizational Role directory entry that has, in the commonName attribute, the distinguished value "securityofficer-n", where n is a numeric value. The significance of the number is solely to differentiate the entries and no order or ranking is implied. There are no spaces in the string.

307. Release Authority Function

a. Two different approaches (shown in Figure 3-1) have been agreed among the Allies for representing Release Authorities in the Allied Directory System, depending on the semantics of Release Authorities in the specifying nation. One approach is to represent the Release Authority function for an organization by having one Release Authority Role Ed. B directory entry (organizationalRole structural object class) associated with the organization. The other method is to represent each person who is a Release Authority for an organization by a Release Authority Person Ed. A directory entry (releaseAuthorityPersonA structural object class) under (i.e., named with respect to) the organization's directory entry.

b. The value "release authority" shall be the distinguished value in the commonName (naming) attribute in a Release Authority Role Ed. B directory entry.

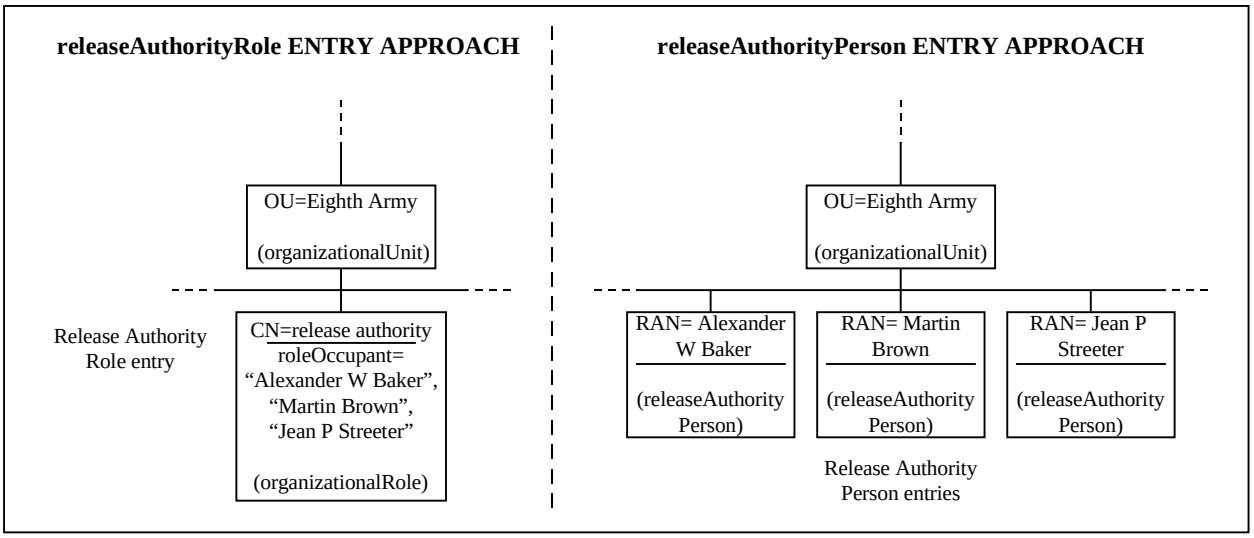

Figure 3-1
Methods of Representing Release Authorities

308. ACP 127 Users

a. In support of the ACP 127 Interworking application, two different approaches, illustrated in Figure 3-2, have been developed for representing ACP 127 users, i.e., PLAs, in the Allied Directory System, depending on the national view concerning integration of ACP 127 information with other information in the DIT. A nation may choose which method is uses in its own DIT subtree to capture PLA information; however, a national schema should support the elements of both methods in order to be able to handle PLA information that may be represented differently in other nations' DIT subtrees.

b. One method is to place PLA-related information in Organizational Unit Ed. A directory entries in the same subtrees as the information for the other applications (i.e., "share" the entries). In this case, the plaUser auxiliary object class shall be used to store the PLA and Routing Indicator (RI) in the organizational entries in the Allied Directory System. This allows the organizational subtree to be searched to find the PLA and RI information.

c. The other approach is to have separate subtrees in the DIT for PLA-related directory entries (e.g., Organizational PLA entries) and for directory entries supporting the other applications. For example, see the U.S. Top-level DIT in Annex B. Using this approach, from the ACP 127 domain, the gateway will search a PLA subtree for an associated Organizational Unit entry where an O/R address is found. From the MMHS domain to the ACP 127 domain, the Organizational Unit Ed. A entry shall have an associated PLA name which can be put in the domain-defined attribute field of the gateway address. RI information will be contained in a directory in the ACP 127 domain. Its inclusion in the X.500 Directory is a national matter.

d. Note that PLA is called Signal Address (SA) or Signal Message Address (SMA) by some nations and international or multinational organizations. Registered PLA is equivalent to SA or SMA. In this ACP, the attribute “longTitle” is defined for storing the spelled out (long form) of a PLA, SA, or SMA.

e. The purpose of the plasServed attribute is to provide the list of PLAs accessible through a gateway. It is necessary for this information to be provided by the Directory so that the X.400 address to route a message to that PLA can be created. This is of particular importance for mobile units such as ships where the gateway via which it is accessible can change. This attribute is also used to route from other types of network to ACP 127.

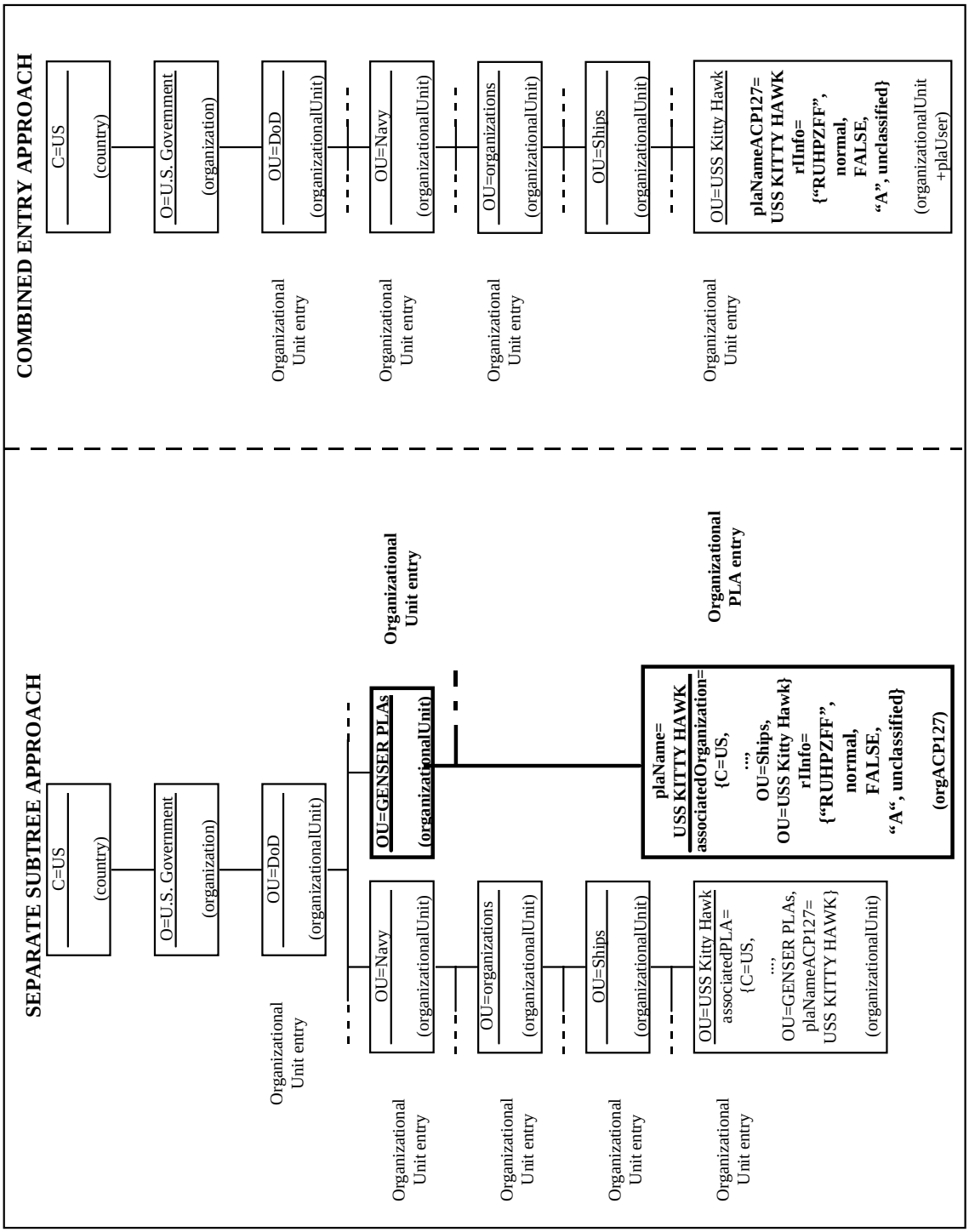

Figure 3-2
Methods of ACP 127 Interworking

309. Interconnected Telecommunication Networks

a. There is a requirement in any military voice switching network to integrate several different tactical and strategic systems. The resulting network provides support to strategic,

operational, and tactical level users. The strategic switching network provides a primary telecommunication service for strategic level users, while a tactical telecommunication network provides a primary service for operational and tactical level users. Access codes provide the means of achieving connectivity between the different types of telecommunications networks.

b. In some cases, there may be more than one route from one network to another, which may involve transiting through an intermediate network. Consequently, a number of different access codes would need to be dialed to achieve connectivity. Additionally, access codes could vary according to the locality of the network. Figure 3-3 gives an example of a number of interconnected strategic (Public Telephone Network, Network A and Local Headquarters (HQ) network) and tactical networks (B, C and D) and their associated access codes.

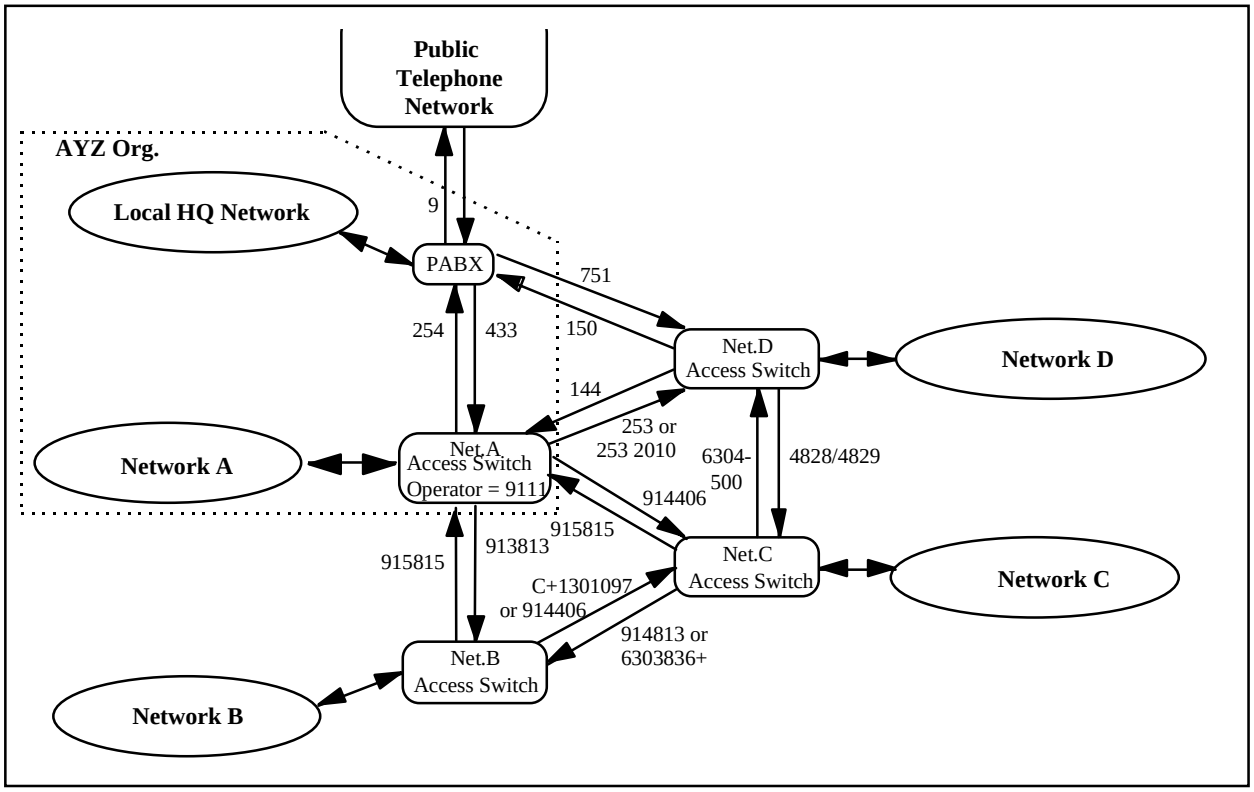

Figure 3-3
Interconnected Strategic and Tactical Networks Example

c. In order to manage the various access codes efficiently, Access Switch managers are responsible for those access codes that provide connectivity to adjacent network access switches. Hence, a set of subtrees within the DIT can be constructed that depict how one network can be reached from another; for example, Figure 3-4 depicts the access codes requirement of Network A to Network B (and vice versa) in Figure 3-3.

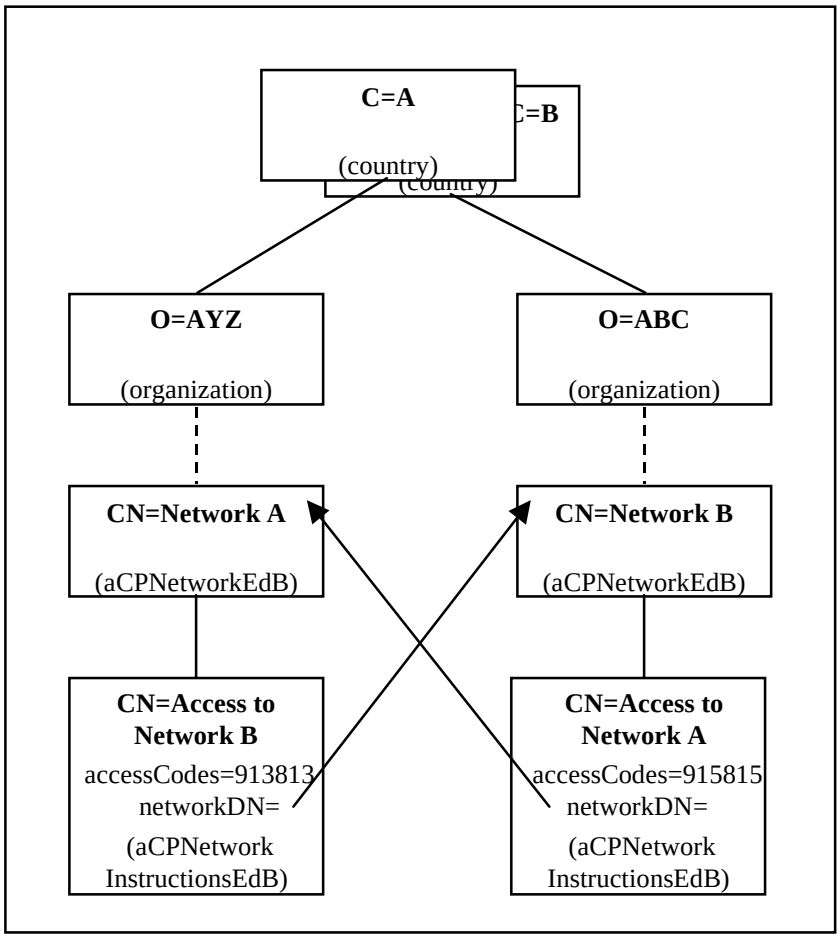

Figure 3-4
DIT Subtree Structure for Network A to Network B Access (and vice versa)

d. For completeness, Figure 3-5 depicts the total access code requirement for Figure 3-3. Although, in principle, the entries refer to “Access to” adjacent networks, the administrator may wish to include “Access to” non-adjacent networks (as denoted by a ‘*’ in Figure 3-5). In considering access between networks they can be considered as either being individual networks or can be associated with a locality, e.g., a HQ, where the user may not know on which network he resides, but knows the HQ he is in and the network or locality he wishes to access. Hence, there are four permutations for the use of access codes, either between networks, localities or both:

- network to locality
- network to network

- locality to network
- locality to locality

e. A user accessing the Allied Directory needs to be able to find the telephone number of the called party (the default being the operator), the access to the network that the called party resides upon, and any special instructions required to complete the connection. Instructions are especially important when transiting across networks that require a special instruction, like “wait for second dial tone, then dial extension”.

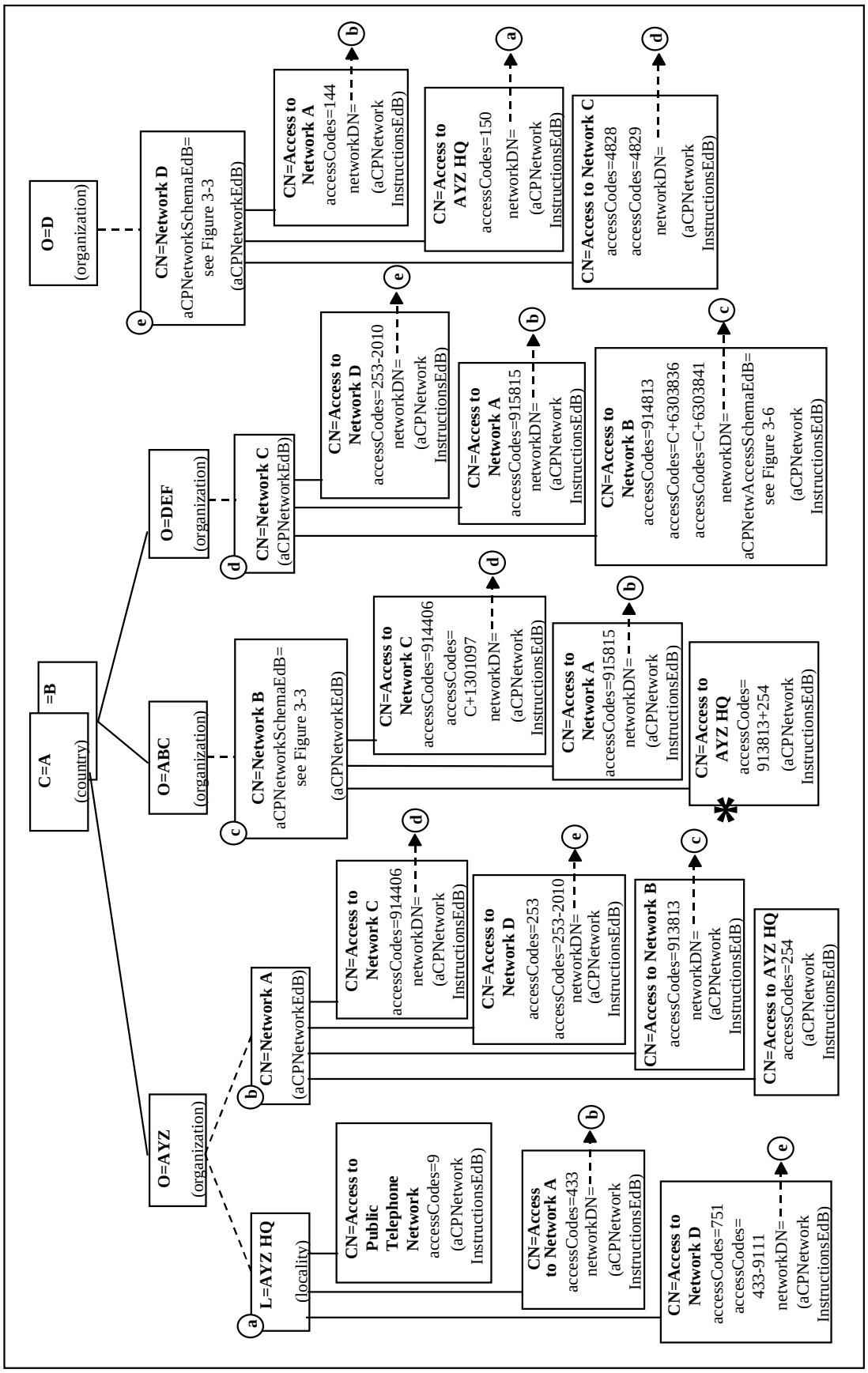

Figure 3-5
DIT Subtree Structure for Network Access Information

f. In support of providing information on telecommunications networks, two types of directory entries are defined:

- Network Ed. B
- Network Instructions Ed. B

g. Network Ed. B entries contain information about the different supported networks. They have subordinated entries that define the access instructions of how to reach other networks.

h. A Network Instructions Ed. B directory entry contains the instructions about how to reach other networks or localities from the entry above in the DIT (see Figure 3-4). When the access to another network is different from different locations, a Locality entry may have subordinated Network Instructions Ed. B directory entries.

i. Note that the new "Ed. B" entry types replace the Network and Network Instructions entry types. Also, the new entry types are based on new object classes: aCPNetworkEdB and aCPNetworkInstructionsEdB, which replace the network and networkInstructions object classes.

j. A number of attributes are used in association with the aCPNetworkEdB/aCPNetworkInstructionsEdB structural object classes as follows.

(1) In a Network Instructions Ed. B entry, the commonName attribute contains the distinguished value “Access to x”, where x is the name of the network or locality for adjacent or non-adjacent networks.

(2) The networkDN attribute value contains the full DN of a NetworkEd. B entry and may be used to reference the entry for the network from another entry. This information is particularly useful where there are too many non-adjacent networks to give instructions for all of them or the instructions for accessing a non-adjacent network change frequently. For example, during the military operation being performed by the CTF that owns the Network C, an advancing force might move across an international boundary. If connection to the Public Telephone Network of the new country is added to Network C, new alternative paths could become available that require the use of access codes appropriate to that Public Telephone Network.

(3) The aCPNetworkSchemaEdB attribute value in the Network Ed. B entry is a graphical representation of a network. It describes the structure of the network and details the rules associated with that network, such as the availability for access to a Public Telephone Network and any details of its elements of service. A possible value could be the diagram in Figure 3-3 which could be included in any or all of the Network Ed. B directory entries in Figure 3-5. Note that the aCPNetworkSchemaEdB attribute type replaces the networkSchema attribute type, in order to employ a different format for the graphics.

(4) The aCPNetwAccessSchemaEdB attribute value in the Network Instructions Ed. B entry is used to present, in a graphical/tabular form, the different connection options between the pair of network interconnections. An example of a tabular description of the interconnection of two networks is given in Figure 3-6. Another use for the aCPNetwAccessSchemaEdB attribute is to take advantage of the Network Instructions Ed. B entry being specific to one other network in order to make it easier for the user to locate the information necessary for a particular connection. Note that the aCPNetwAccessSchemaEdB attribute type replaces the accessSchema attribute type, in order to employ a different format for the graphics.

(5) The accessCodes attribute value is used to hold the actual codes used to reach one network from another. These values may also be shown in the accessSchema attribute. It also contains additional instructions, such as, when it is necessary to wait for an operator to connect, then followed by dialing the desired extension number.

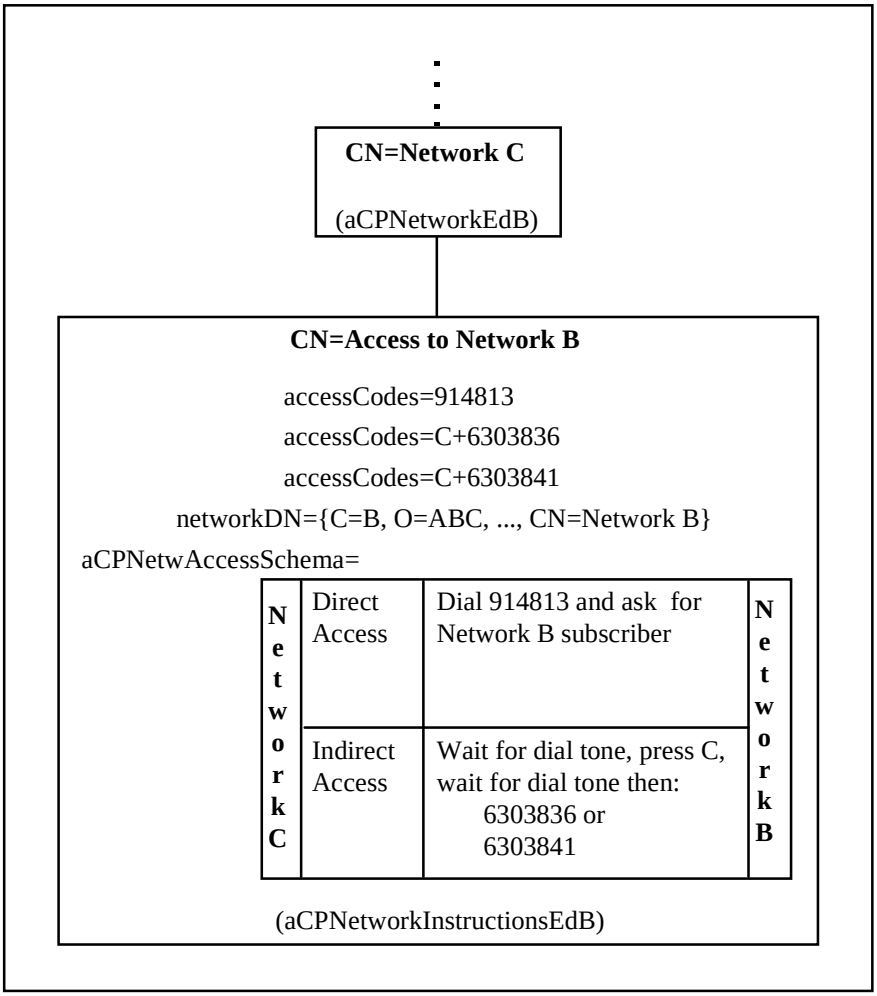

Figure 3-6
Example of an aCPNetwAccessSchemaEdB for Network B

310. Use of the seeAlso Attribute

The correct use of the seeAlso attribute can benefit Allied Directory System users. Conversely poor use of the attribute can have an adverse effect on performance of the Allied Directory System and create frustration for users and additional burden for directory administrators. It is the responsibility of the directory administrator to ensure that the seeAlso attribute values are valid and do not point to non-existent directory entries. The procedural recommendations for the use of the seeAlso attribute in each of the relevant directory entry types are given below. In all cases, the seeAlso attribute is optional.

a. Application Entity Ed. A

The seeAlso attribute for the Application Entity may be used to point to other Application Entity Ed. A directory entries. Specific types of application entity covered separately include DSA, MLA, MHS UA, etc.

b. Device Ed. A

The seeAlso attribute for the Device may be used to point to other Device Ed. A directory entries. Examples would be pointers to printers with similar capabilities.

c. DSA Ed. A

The seeAlso attribute for the DSA may be used to point to other DSA Ed. A directory entries. For example, it may point to a DSA providing back-up to this DSA.

d. MHS Distribution List

The seeAlso attribute for the MHS Distribution List may be used to point to other MHS Distribution List directory entries. No specific use has been identified at this time.

e. MHS Message Store Ed. A

The seeAlso attribute for the MHS Message Store Ed. A may be used to point to other MHS Message Store Ed. A directory entries. No specific use has been identified at this time.

f. MHS Message Transfer Agent Ed. A

The seeAlso attribute for the MHS Message Transfer Agent Ed. A may be used to point to other MHS Message Transfer Agent Ed. A directory entries. The other directory entries could be for MTAs with the same type of function in a domain, such as, backbone MTAs that serve the same geographic area.

g. MHS User Agent

The seeAlso attribute for the MHS User Agent may be used to point to other MHS User Agent directory entries. No specific use has been identified at this time.

h. Organization Ed. B

The seeAlso attribute for the Organization Ed. B may be used to point to other Organization Ed. B directory entries. Whether this would be useful is questionable because of the high level of organizations in the DIT, for example, NATO.

i. Organizational Person Ed. B

The seeAlso attribute for the Organizational Person Ed. B may be used to point to other Organizational Person Ed. B directory entries. These other Organizational Person Ed. B directory entries shall be from the same organization or organizational unit, physically close, or have similar functional duties to the source entry person. A possible use is a pointer to another identity for an organizational person, such as, in a combined domain. It could also be used to point to the Organizational Role Ed. B directory entries which designate the organizational person as a role occupant.

j. Organizational Role Ed. B

The seeAlso attribute for the Organizational Role Ed. B may be used to point to other Organizational Role Ed. B directory entries. These other Organizational Role Ed. B directory entries shall be from the same organization or organizational unit, physically close, or have similar functional duties to the source entry.

k. Organizational Unit Ed. B

The seeAlso attribute for the Organizational Unit Ed. B may be used to point to other Organizational Unit Ed. B directory entries. These other Organizational Unit Ed. B directory entries shall be from the same organization, physically close to, or have similar functional duties to that of the source entry. A possible use is a pointer to a portion of an organizational unit which has been deployed and is part of a combined domain.

l. Address List Ed. A

The seeAlso attribute for the Address List Ed. A may be used to point to other Address List Ed. A directory entries. No specific use has been identified at this time.

m. Application Process

The seeAlso attribute for the Application Process may be used to point to Application Entity Ed. A and other Application Process directory entries. No specific use has been identified at this time.

n. Group of Names

The seeAlso attribute for the Group of Names may be used to point to other Group of Names directory entries. No specific use has been identified at this time.

o. Locality

The seeAlso attribute for the Locality may be used to point to other Locality directory entries. No specific use has been identified at this time.

p. Messaging Gateway Ed. A

The seeAlso attribute for the Messaging Gateway Ed. A may be used to point to other Messaging Gateway Ed. A directory entries. These other Messaging Gateway Ed. A directory entries shall have the same capability, e.g., translation between ACP 127 and ACP 123 messaging networks, and belong to the same domain.

q. MLA Ed. A

The seeAlso attribute for the MLA Ed. A may be used to point to other MLA Ed. A directory entries. The attribute could point to another MLA responsible for the same mail lists.

r. Release Authority Role Ed. B

The seeAlso attribute for the Release Authority Role may be used to point to other Release Authority Role Ed. B and Organizational Role Ed. B directory entries. No specific use has been identified at this time.

SECTION II

ENTRY AND ATTRIBUTE POPULATION AND USAGE

311. Population Requirements and Guidelines for Various Types of Communications

a. This section is intended for administrators who are planning for or are populating the directory entries in the Allied Directory System. Population refers to the directory entries and attributes for which values should be made available in the Allied Directory to support given user applications. The minimal subset of the Common Content that needs to be populated for various communication applications is stated in this section. (See Annex B for specification of the Common Content.) The types of applications for which population requirements are stated are:

- e-mail communication (non-X.400)
- Secure Multi-purpose Internet Mail Extension (S/MIME)
- commercial MHS communication

- MMHS communication
- communication between MMHS users and ACP 127 users
- traditional communications (e.g., telephone, facsimile, and postal mail)

b. Table 3-1 indicates the directory entries required. Table 3-2 indicates the required auxiliary object classes for directory entries. Tables 3-3 through 3-21 indicate the associated attributes for which values are necessary to support each application.

c. For e-mail communication (non-X.400), the directory entries and attributes shall contain the common name and e-mail (RFC 822) address.

d. For S/MIME communication, the directory entries and attributes shall contain the common name, e-mail (RFC 822) address, and user certificate.

e. For commercial Message Handling System (i.e., civilian X.400) communication, the directory entries and attributes shall contain the information necessary for performing the core functions of a messaging system. These functions include, but are not restricted to: addressing, routing, expanding address lists, and directory access.

f. For MMHS and e-mail services with confidentiality and digital signature features, the directory entries and attributes shall contain the information necessary for performing the core functions of a secure messaging system. These functions include: addressing, routing, securing a message, translating from one type of messaging protocol into another, expanding address lists, and directory access.

g. For interworking between the ACP 127 and MMHS systems, the directory entries and attributes shall contain the information necessary to identify and characterize ACP 127 users and to utilize the gateway(s) between the two systems.

h. In order to support traditional communication services, such as, telephone, facsimile, and postal mail, the directory entries and their associated attributes shall contain the information necessary for human users to look up someone else's information by providing a common name of an organizational person or organizational role, or the organizational unit name of an organization. The directory serves as a repository of this information, and after the user gets the information from the directory, the rest of the communication takes place using the traditional communications network.

i. Table 3-1 indicates, for each application, the directory entries that are necessary for Allied communication whether specified by the standards or in the Abstract Syntax Notation One (ASN.1) definitions in this ACP. If the directory entry is required, then it is indicated by a "•" to highlight that the Allied Directory shall contain directory entries of that type.

Table 3-1
Population of Directory Entries for Applications

Entry Type	E-MAIL	S/MIME	Com-mercial MHS	MMHS	ACP 127 Inter-working	Tradi-tional Com-munica-tions
1. Address List Ed. A				•	•	
2. Application Entity Ed. A	•	•	•	•	•	•
3. Certification Authority Ed. B		•		•		
4. CRL Distribution Point		•		•		
5. DSA Ed. A	•	•	•	•	•	•
6. Group of Names		•		•		•
7. Messaging Gateway Ed. A	•	•	•[2]	•[2]	•	
8. MHS Message Store Ed. A			•[2]	•[2]		
9. MHS Message Transfer Agent Ed. A			•[2]	•[2]		
10. MLA Ed. A				•[2]		
11. Organizational Person Ed. B	•	•	•	•		•
12. Organizational PLA					•[1]	
13. Organizational Role Ed. B	•	•	•	•		•
14. Organizational Unit Ed. B		•	•	•	•	•
15. PLA Collective					•	
16. Release Authority Person Ed. A				•[3]		
17. Release Authority Role Ed. B				•[3]		
18. Task Force PLA					•	
19. Tenant PLA					•	

[1] The requirement shown applies only when the "separate subtree" method is employed, as described in paragraph 308.

[2] These entries must be populated where the messaging system is built to make use of them.

[3] One of Release Authority Person Ed. A or Release Authority Role Ed. B needs to be populated.

j. In addition, entries for Country, Organization, Organizational Unit, and Locality may need to be populated in order to provide structure for a nation's DIT.

k. Table 3-2 indicates the auxiliary object classes, which are optional in the Common Content (i.e., a class that is added to an entry type using a content rule; see Annex B), that some applications require for a certain entry type. If the auxiliary object class is required by an

application, then it is indicated by a "•" to highlight that the auxiliary object class's object identifier shall be included in the object class attribute in the directory entry.

Table 3-2
Auxiliary Object Classes Required in Directory Entries for Applications

Entry Type and Auxiliary Object Classes	E-MAIL	S/MIME	Commercial MHS	MMHS	ACP 127 Interworking	Traditional Communications
1. Address List Ed. A						
distributionCodesHandled						
mhs-user				•		
plaUser					•[1]	
securePkiUser				•		
ukms						
2. Certification Authority Ed. B[2]						
pkiCA		•		•		
3. DSA Ed. A						
securePkiUser	•	•	•	•	•	•
4. Messaging Gateway Ed. A						
securePkiUser		•		•		
ukms						
5. MHS Message Store Ed. A						
securePkiUser				•		
6. MHS Message Transfer Agent Ed. A						
securePkiUser				•		
7. Organizational Person Ed. B						
distributionCodesHandled						
mhs-user			•	•		
otherContactInformation						•
securePkiUser		•[3]		•		
ukms						

Table 3-2
Auxiliary Object Classes Required in Directory Entries for Applications

Entry Type and Auxiliary Object Classes	E-MAIL	S/MIME	Com-mercial MHS	MMHS	ACP 127 Inter-working	Tradi-tional Com-munica-tions
8. Organizational Role Ed. B						
pkiCA						
distributionCodesHandled						
mhs-user			•	•		
otherContactInformation						•
securePkiUser		•[3]		•		
ukms						
9. Organizational Unit Ed. B						
distributionCodesHandled						
mhs-user			•	•		
otherContactInformation						•
plaUser					•[1]	
securePkiUser		•[3]		•		
ukms						

[1] The requirement shown applies only when the "combined entry" method is employed, as described in paragraph 308.
[2] Requirements for auxiliary object classes, other than pkiCA, are the same as for the entry type (Organization Ed. B, Organizational Role Ed. B, Organizational Unit Ed. B, or Application Entity Ed. A) as the nation is using for representing CAs.
[3] S/MIME requires population of pkiUser which is a superclass of securePkiUser.

l. Tables 3-3 through 3-21 indicate, for each application, the directory entry's attributes that are necessary for Allied communication including those mandated by the standards or in the ASN.1 definitions in this ACP. If the attribute is required for any of these reasons, then it is indicated by a "•" to highlight that the attribute value shall be "populated" (i.e., the attribute has a value). Attributes listed under the directory entries are a combination of the attributes included in the entry type's structural object class (including those attributes included in the base object class and those attributes inherited from superclasses) and the auxiliary object classes and additional attributes added to that entry. All attributes that require values shall include a non-null value. Exceptions are:

- attribute values for which a value does not exist
- attributes required by the standards that are not used by the ACP 133
- attributes where population is prohibited by the user's security policy

m. Specific exceptions to populating the attributes are highlighted in the following paragraphs.

Table 3-3
Population of Address List Ed. A

Attribute	E-MAIL	S/MIME	Commercial MHS	MMHS	ACP 127 Interworking	Traditional Communications
1. commonName				•	•	
2. copyMember[1]				•	•	
3. description				•	•	
4. mhs-dl-submit-permissions				•	•	
5. mhs-or-addresses				•	•	
6. mhs-or-addresses-with-capabilities[2]				•	•	
7. owner				•	•	
8. member[1]				•	•	
9. userCertificate				•	•	

[1] An Address List entry shall have values in the member attribute or copyMember attribute or both.

[2] Applies only if there are multiple O/R addresses in the entry or if there is a need to associate a security label with an O/R address.

Table 3-4
Population of Application Entity Ed. A

Attribute	E-MAIL	S/MIME	Commercial MHS	MMHS	ACP 127 Interworking	Traditional Communications
1. commonName	•	•	•	•	•	•
2. presentationAddress	•	•	•	•	•	•

n. Table 3-5 includes information used to send messages to a CA represented by a Certification Authority Ed. B entry. This table indicates for each application, the population requirements for the attributes in the pkiCA auxiliary object class, in addition to the requirements for the Organization Ed. B, Organizational Role Ed. B, Organizational Unit Ed. B, or Application Entity Ed. A entry type of which the Certification Authority Ed. B directory entry type is a special case.

Table 3-5
Population of Certification Authority Ed. B[1]

Attribute	E-MAIL	S/MIME	Commercial MHS	MMHS	ACP 127 Interworking	Traditional Communications
1. authorityRevocationList		•		•		
2. cACertificate		•		•		
3. certificateRevocationList		•		•[2]		
4. crossCertificatePair[3]		•		•		

[1] The attributes in this table are in addition to whatever attributes may also be populated in the entry, as a result of the structural and other object classes to which the entry also belongs.

[2] Alternatively, certificateRevocationList may be populated in a CRL Distribution Point entry.

[3] The forward certificate within the cross certificate pair shall be present; the reverse certificate should be present, if it is available.

Table 3-6
Population of CRL Distribution Point

Attribute	E-MAIL	S/MIME	Commercial MHS	MMHS	ACP 127 Interworking	Traditional Communications
1. authorityRevocationList		•		•		
2. certificateRevocationList		•		•		
3. commonName		•		•		

Table 3-7
Population of DSA Ed. A

Attribute	E-MAIL	S/MIME	Commercial MHS	MMHS	ACP 127 Interworking	Traditional Communications
1. commonName	•	•	•	•	•	•
2. presentationAddress	•	•	•	•	•	•
3. supportedAlgorithms	•	•	•	•	•	•
4. userCertificate	•	•	•	•	•	•

Table 3-8
Population of Group of Names

Attribute	E-MAIL	S/MIME	Commercial MHS	MMHS	ACP 127 Interworking	Traditional Communications
1. commonName		•		•		
2. member		•		•		

o. In Table 3-9, each of the columns represents a level of service that can be implemented in a gateway being used for interworking between MMHS domains and other messaging domains (i.e., e-mail, commercial MHS, MMHS, and ACP 127).

Table 3-9
Population of Messaging Gateway Ed. A

Attribute	E-MAIL	S/MIME	Commercial MHS	MMHS	ACP 127 Interworking	Traditional Communications
1. commonName	•	•	•	•	•	
2. mhs-or-addresses			•	•	•	
3. mhs-or-addresses-with-capabilities[1]			•	•	•	
4. plasServed					•	
5. presentationAddress	•	•	•	•	•	
6. rfc822Mailbox	•	•				
7. supportedAlgorithms		•		•	•	
8. userCertificate		•		•	•	

[1] Applies only if there are multiple O/R addresses in the entry or if there is a need to associate a security label with an O/R address.

Table 3-10
Population of MHS Message Store Ed. A

Attribute	E-MAIL	S/MIME	Commercial MHS	MMHS	ACP 127 Interworking	Traditional Communications
1. commonName			•	•		
2. presentationAddress			•	•		

Table 3-11
Population of MHS Message Transfer Agent Ed. A

Attribute	E-MAIL	S/MIME	Commercial MHS	MMHS	ACP 127 Interworking	Traditional Communications
1. commonName			•	•		
2. presentationAddress			•	•		
3. supportedAlgorithms				•		
4. userCertificate				•		

Table 3-12
Population of MLA Ed. A

Attribute	E-MAIL	S/MIME	Commercial MHS	MMHS	ACP 127 Interworking	Traditional Communications
1. commonName				•		
2. presentationAddress				•		
3. supportedAlgorithms				•		
4. userCertificate				•		

Table 3-13
Population of Organizational Person Ed. B

Attribute	E-MAIL	S/MIME	Commercial MHS	MMHS	ACP 127 Interworking	Traditional Communications
1. aCPMobileTelephoneNumber						•[1]
2. commonName	•	•	•	•		•
3. dnQualifier	•[1]	•[1]	•[1]	•[1]		•[1]
4. facsimileTelephoneNumber						•[1]

Table 3-13
Population of Organizational Person Ed. B

Attribute	E-MAIL	S/MIME	Commercial MHS	MMHS	ACP 127 Interworking	Traditional Communications
5. mhs-or-addresses			•	•		
6. mhs-or-addresses-with-capabilities[2]			•	•		
7. militaryFacsimileNumber						•[1]
8. militaryTelephoneNumber						•[1]
9. organizationalUnitName	•	•	•	•		•
10. postalAddress						•
11. proprietaryMailboxes	•[1]					
12. rfc822Mailbox	•	•				
13. secureFacsimileNumber						•[1]
14. secureTelephoneNumber						•[1]
15. supportedAlgorithms		•		•		
16. telephoneNumber						•[1]
17. userCertificate		•		•		

[1] Population of the attribute is dependent upon the user having a value for the attribute (e.g., if the user does not have a mobile telephone number then an attribute value shall not be included in the attribute).

[2] Applies only if there are multiple O/R addresses in the entry or if there is a need to associate a security label with an O/R address.

Table 3-14
Population of Organizational PLA

Attribute	E-MAIL	S/MIME	Commercial MHS	MMHS	ACP 127 Interworking [1]	Traditional Communications
1. associatedOrganization					•	
2. countryName					•[2]	

Table 3-14
Population of Organizational PLA

Attribute	E-MAIL	S/MIME	Com-mercial MHS	MMHS	ACP 127 Inter-working [1]	Tradi-tional Com-munica-tions
3. effectiveDate					•[2]	
4. localityName					•[2]	
5. longTitle					•[2]	
6. plaNameACP127					•	
7. remarks					•[2]	
8. rIInfo					•[3]	

[1] The requirements shown for this application apply when the "separate subtree" method is employed, as described in paragraph 308.

[2] These attributes are used when the directory is used to store ACP 117 information (i.e., publish ACP 117).

[3] This attribute is populated when the directory implementation supports use of RI information.

Table 3-15
Population of Organizational Role Ed. B

Attribute	E-MAIL	S/MIME	Com-mercial MHS	MMHS	ACP 127 Inter-working	Tradi-tional Com-munica-tions
1. aCPMobileTelephoneNumber						•[1]
2. commonName	•	•	•	•		•
3. facsimileTelephoneNumber						•[1]
4. mhs-or-addresses			•	•		
5. mhs-or-addresses-with-capabilities[2]			•	•		
6. militaryFacsimileNumber						•[1]
7. militaryTelephoneNumber						•[1]
8. roleOccupant	•	•	•	•		•
9. postalAddress						•

Table 3-15
Population of Organizational Role Ed. B

Attribute	E-MAIL	S/MIME	Commercial MHS	MMHS	ACP 127 Interworking	Traditional Communications
10. proprietaryMailboxes	•[1]					
11. rfc822Mailbox	•	•				
12. secureFacsimileNumber						•[1]
13. secureTelephoneNumber						•[1]
14. supportedAlgorithms		•		•		
15. telephoneNumber						•[1]
16. userCertificate		•		•		

[1] Population of the attribute is dependent upon the user having a value for the attribute (e.g., if the user does not have a mobile telephone number then an attribute value shall not be included in the attribute).

[2] Applies only if there are multiple O/R addresses in the entry or if there is a need to associate a security label with an O/R address.

Table 3-16
Population of Organizational Unit Ed. B

Attribute	E-MAIL	S/MIME	Commercial MHS	MMHS	ACP 127 Interworking	Traditional Communications
1. aCPMobileTelephoneNumber						•[2]
2. associatedPLA					•[1]	
3. facsimileTelephoneNumber						•[2]
4. mhs-or-addresses			•	•		
5. mhs-or-addresses-with-capabilities[3]			•	•		
6. militaryFacsimileNumber						•[2]
7. militaryTelephoneNumber						•[2]
8. organizationalUnitName		•	•	•		•

Table 3-16
Population of Organizational Unit Ed. B

Attribute	E-MAIL	S/MIME	Com-mercial MHS	MMHS	ACP 127 Inter-working	Tradi-tional Com-munica-tions
9. plaNameACP127					•[4]	
10. postalAddress						•
11. rfc822Mailbox		•				
12. secureFacsimileNumber						•[2]
13. secureTelephoneNumber						•[2]
14. supportedAlgorithms		•		•		
15. telephoneNumber						•[2]
16. userCertificate		•		•		

[1] The requirements shown for this application apply when the "separate subtree" method is employed, as described in paragraph 308.

[2] Population of the attribute is dependent upon the user having a value for the attribute (e.g., if the user does not have a mobile telephone number then an attribute value shall not be included in the attribute).

[3] Applies only if there are multiple O/R addresses in the entry or if there is a need to associate a security label with an O/R address.

[4] The requirements shown for this application apply when the "combined entry" method is employed, as described in paragraph 308.

p. A PLA Collective directory entry shall be used when a pointer is necessary to check on the validity of a PLA, e.g., for Type Organization Collectives.

Table 3-17
Population of PLA Collective

Attribute	E-MAIL	S/MIME	Com-mercial MHS	MMHS	ACP 127 Inter-working [1]	Tradi-tional Com-munica-tions
1. associatedAL					•	
2. plaNameACP127					•	

[1] The requirements shown for this application apply when the "separate subtree" method is employed, as described in paragraph 308.

Table 3-18
Population of Release Authority Person Ed. A

Attribute	E-MAIL	S/MIME	Com-mercial MHS	MMHS	ACP 127 Inter-working [1]	Tradi-tional Com-munica-tions
1. releaseAuthorityName				•		
2. supportedAlgorithms				•		
3. userCertificate				•		

q. Table 3-19 includes information used to send messages to a Release Authority, which is represented by a Release Authority Role Ed. B entry.

Table 3-19
Population of Release Authority Role Ed. B

Attribute	E-MAIL	S/MIME	Com-mercial MHS	MMHS	ACP 127 Inter-working	Tradi-tional Com-munica-tions
1. commonName	•		•	•		•
2. facsimileTelephoneNumber						•[1]
3. mhs-or-addresses			•	•		
4. mhs-or-addresses-with-capabilities[2]			•	•		
5. militaryFacsimileNumber						•[1]
6. militaryTelephoneNumber						•[1]
7. mobileTelephoneNumber						•[1]
8. roleOccupant	•		•	•		•
9. postalAddress						•
10. proprietaryMailboxes	•[1]					
11. rfc822Mailbox	•					
12. secureFacsimileNumber						•[1]
13. secureTelephoneNumber						•[1]
14. supportedAlgorithms				•		
15. telephoneNumber						•[1]
16. userCertificate				•		

[1] Population of the attribute is dependent upon the user having a value for the attribute (e.g., if the user does not have a mobile telephone number, then an attribute value shall not be included in the attribute).

[2] Applies only if there are multiple O/R addresses in the entry or if there is a need to associate a security label with an O/R address.

Table 3-20
Population of Task Force PLA

Attribute	E-MAIL	S/MIME	Com-mercial MHS	MMHS	ACP 127 Inter-working [1]	Tradi-tional Com-munica-tions
1. associatedAL					•	
2. plaNameACP127					•	

[1] The requirements shown for this application apply when the "separate subtree" method is employed, as described in paragraph 308.

Table 3-21
Population of Tenant PLA

Attribute	E-MAIL	S/MIME	Com-mercial MHS	MMHS	ACP 127 Inter-working	Tradi-tional Com-munica-tions
1. hostOrgACP127					•	
2. plaNameACP127					•	

SECTION III

REGISTRATION

312. Registration Requirements

The following objects need to be registered to ensure that they are unique with a global context of the Allied Directory:

- technical object identifiers
- directory DNs
- other information stored in the directory, e.g., addresses

313. Technical Object Identifier

a. Object identifiers provide a unique reference to the definition of technical objects. This includes technical objects which are specific to the directory such as object class and attribute definitions, as well as technical objects which have wider relevance such as certificate policy identifiers. Other applications such as Open Systems Interconnection (OSI) management and messaging also make use of object identifiers to reference technical definitions.

b. Object identifiers for standard technical definitions are allocated in the standard where they are defined (e.g., X.500 allocates object identifiers for directory object classes and attributes defined in that standard).

c. Object identifiers for new schema definitions for object classes, attributes, name forms, etc., for the Allied Directory are defined in this ACP (see Annex B) under the object identifier:

{ joint-iso-ccitt(2) country(16) us(840) organization(1) gov(101) dod(2) ds(2) }

d. National or other new schema definitions outside the scope of this ACP are allocated object identifiers under the appropriate national or international object identifier registration scheme.

314. Distinguished Name

a. A DN is a sequence of naming attributes which uniquely identify an object which may be represented by an entry in the directory. Objects that may be identified using a distinguished name include organizational units, people, roles, address lists, devices, application entities, and release authorities. A distinguished name is used as the primary "key" to locate an entry in the Allied Directory. In addition, distinguished names are used to identify the subject of an X.509 public key certificate.

b. The naming attributes which form a DN are organized in a hierarchy reflecting the DIT with a name lower in the tree identified relative to its parent entry by adding RDN attributes to the parent's DN.

c. Before an entry is created for an object in the directory (or a certificate created for that object) it must be allocated a DN which is unique. The allocation of a distinguished name in the Allied Directory is the responsibility of the Registration Authority for the Service, agency, or command to which the named object belongs. A registration authority may delegate responsibility of directory distinguished name registration for subtrees within its domain to Sub-Registration Authorities. A registration authority (or sub-registration authority) may also take on responsibility for registration of other identifiers including technical object identifiers and addresses (see below).

d. The DNs used at the top levels of Allied directory domains are given in Annex B.

e. The registered DNs relevant to the Allied Directory may be disseminated through the directory.

315. General Registration Requirements

a. The directory can be used to store addressing and other related information. As with DNs these addresses need to be unique within the global context and hence must be allocated under a registration scheme. Examples of information requiring registration are X.400 MHS Addresses (including Private Management Domain (PRMD) identifiers), OSI network addresses, and Internet Protocol addresses.

b. The specific registration requirements for the registration of information such as addresses is dependent on the type of communication or application service to which the information applies, and is hence outside the scope of this ACP. However, objects which are allocated DNs commonly also require addresses (e.g., X.400 addresses) and, hence, the various registration functions should be coordinated using coherent registration procedures.

c. Common Allied registration guidelines are recommended. This should cover procedures for coordination, dissemination, and ratification of registration information, such as:

- technical objects identifiers defined for Allied use
- DNs used in the Allied context
- X.400 addresses

SECTION IV

SHADOWING

316. Shadowing Policy

a. A Shadowing Agreement Checklist is initiated by the administrator of the supplier DSA, who administers the information requiring shadowing. The Shadowing Agreement Checklist is filled out and provided to the consumer DSA administrator for completion and agreement. The Shadowing Agreement is reviewed and approved by the Directory Services Manager. The agreement shall state the protection provided to shadowed information. Also, when agreement involves secondary shadowing, the Shadowing Agreement Checklist is reviewed and approved by the DSA Administrator of the Master DSA. Annex E gives an example of a Shadowing Agreement Checklist, including the standard X.500 shadowing agreement parameters.

b. Directory information that is provided to the Allied Directory System from national directories may be shadowed, and individual entries within this information may be incomplete. Thus, users may not find what they are looking for and require access to the master or a complete

replicated entry. In a directory system unconstrained by access controls, users would be able to satisfy the request by chaining from the Border DSA into the national directory. However, this situation may not be permitted. In order to satisfy one nation's directory queries of another nation's Border DSA, consideration should be given to the way in which replicated data is marked. The options are that the data may be marked as a master or copy. If it is a copy, it may be marked as incomplete. If it is marked as incomplete, it implies that chaining is permitted into the directory that contains the complete entry. This may be a national DSA or another Border DSA. How data is marked should be specified within the allied Service Level Agreements (SLAs).

SECTION V

DIRECTORY SYSTEM PERFORMANCE

317. General

The Allied and the supporting national directories, which combine to form an overall directory service capability for the allied forces, must have realistic performance characteristics. Performance can be seen in a number of ways namely: ease of use, robustness, timeliness of service restoration, and speed of access response.

a. Ease of Use

Ease of use is a factor of the system design and the tools presented to the directory user such as click and point, icons, windows, scripts, status messages, etc. This aspect of the system is beyond the scope of this document but will be subject to national system Concepts of Operations (CONOPS), policies, and procurement procedures.

b. Robustness

Robustness deals with product and system reliability and integrity. Again, these will have to be specified in terms of Integrated Logistics Support (ILS) and Life-Cycle Costing (LCC) needs and Mean Time Between Failure (MTBF)/Mean Time To Repair (MTTR) type specifications. This is also beyond the scope of this document.

c. Availability

The goal is to provide 24 by 7 availability of the Allied Directory Service.

d. Service restoration

Service Restoration deals with the recovery time for a single DSA to attain an operational state after switch on or switching the DUAs (and other attached DSAs) to an alternate DSA. This should not exceed five minutes if the DSA is in a strategic environment. In a tactical environment, it should be less than one minute.

e. Speed of Response

(1) For defining the speed of response requirements, the directory system can be seen to provide two types of access characteristics. These are:

- the human access requirements, which deal with organizational information retrieval (such as postal and telecommunications information) via a man-machine interface

- specific system functions (such as MTAs and UAs), which need to resolve for example, names to addresses for message routing. This interface is considered to be a machine-to-machine interface.

(2) Both of the above have performance requirements. However, how these are characterized and presented can be quite different. Underlying the performance of such a large scale system is naturally the individual DSA performance and the links used between them to other DSAs and the accessing DUAs. It is outside the scope of this document to provide specifics of these, except that some general guidelines are provided to assess the capability of a DSA platform and determine its accessibility and performance in a distributed environment.

318. Human Interfaces

a. In terms of specifics, the human interface and its response requirements set the directory performance requirements and thus impose the directory system design.

b. The directory user interface performance requirement is as follows:

(1) All interrogation accesses satisfied in the home DSA shall be performed within three seconds for a ten-kilobyte retrieval.

(2) 95 percent of the intra-domain interrogation accesses shall be satisfied within five seconds for a ten-kilobyte retrieval. Worst case shall not exceed ten seconds.

(3) 90 percent of the inter-domain interrogation accesses shall be satisfied within 15 seconds for a ten-kilobyte retrieval. Worst case shall not exceed 20 seconds.

(4) An update operation to a single entry shall be performed within five seconds.

319. First-level DSAs

Performance requirements for access to first-level DSAs (FLDSA) are derived from the requirement for passing messages according to their precedence/priority in specified times as described in ACP 123 and shown in Table 3-21. All accesses to directories which serve the Message Transfer System (MTS) and the transfer of a message must not jeopardize the messaging throughput requirements. A few guidelines can be given.

a. For any Allied scenario, each FLDSA in the system should route DAP or DSP requests to its adjacent DSA in less than 500 milliseconds.

b. For any Allied scenario, each FLDSA in the system should be able to replicate into its country and direct organizational level entries (to a maximum of 12 entries, e.g., eight Country plus four organization entries) in less than two seconds.

c. For any Allied scenario, each FLDSA in the system which detects failure in protocol operations (DAP, DSP, DISP), should signal its attached ADUA or management center within one second.

d. For any Allied scenario, where any FLDSA fails and goes off line, a standby should be operational within 30 seconds and any reconfiguring of replication agreements achieved in one minute.

e. Each FLDSA in the system should be provided with sufficient processing and storage resource to assemble fragmented Search and List results of 200 entries in less than one second.

f. Each FLDSA in the system should be synchronized to a responsible time source with a maximum deviation of five seconds from other FLDSAs.

320. System Function Access

a. Military Messaging

(1) This type of access serves the allied messaging system's processing entities. These entities are typically messaging UAs, MTAs, MLAs, CAs, Profiling User Agents and Gateways (tactical, security, etc.) that incorporate DUA functions.

(2) Most of the above will access their associated directories for very specific needs such as list expansion, name to address translation or user submission/delivery capability testing. In terms of specifying performance for the combined messaging and directory system, the overall capability is to pass messages according to their precedence/priority in specified times. This is specified in ACP 123. For instance, a Flash (Urgent) message must traverse the allied MTS within three minutes. Therefore, all accesses to the directories which serve the MTS and the transfer of this message must not jeopardize the messaging throughput requirement.

(3) How many accesses to directories will occur along any specific MTS transfer path cannot be accurately determined without hard configuration information, but it is considered that nominally, there could be five directory accesses with a worst case of ten. The total time for these accesses shall be less than 20 percent of the overall message transit time requirement (for Flash messages).

(4) Table 3-22 reflects this for the various message precedence levels. Naturally, only generalized access speeds are provided. For example, for the worst cases (Non-Urgent <= eight hours), it is unlikely for a DSA to take the full 60 seconds if it is locally accessed by the

respective MTA and the information required is contained in it. However, the requirement for servicing Override and Flash messages shall be strictly observed.

Table 3-22
MHS-derived Directory System User Speed of Query Requirements

Military Precedence	MTS Grade of Delivery/Directory Priority	Originator-to-Recipient Time of Delivery	MTS Time of Delivery	Directory Speed of Query Requirement*
OVERRIDE	URGENT/high	3 min.	≤3 min.	2.5 sec.
FLASH		10 min.		
IMMEDIATE	NORMAL/ medium	20 min.	≤20 min.	7.5 sec.
PRIORITY		45 min.		
ROUTINE	NON-URGENT/ low	≤ 8 hours or start of next business day	≤ 8 hours or start of next business day	30 sec.
DEFERRED				

* These values assume that the DUA has already performed a Bind operation with the DSA. If the DUA is not bound, the combined bind and query shall take no more than twice as long as indicated here.

(5) It should be noted that there is no formal way in which an MTA, because of message priority/precedence, will set or test the time a directory query takes. This is a product design and implementation issue. The Allies should seek implementations where the message priority is reflected in the directory access priority in service controls between the MTA and DSA which service that message.

(6) It should also be noted that there is no formal way in which a messaging user can, during the construction of a message, request that the DSA perform directory accesses at a priority in line with the message precedence proposed, unless the precedence field is provided before related Military Messaging User Agent (MMUA) directory accesses are performed and the implementation ties the access priority to the message precedence.

(7) Thus, directory performance levels can be realistically requested only for dealing with message transfer through the MTS from the point of submission.

b. Other Applications

The Allied Directory System will be accessed for other purposes than supporting the messaging function. Examples of functions for which the performance criteria for directory access may be different from the messaging support criteria are:

- authenticating management entities
- distributing certificate revocation lists (CRLs)

321. Performance Characteristics

The following text provides some generalized notes that should be applied in the procurement, design, and operation of the directory systems for both the national systems and the shared/combined systems.

a. DUA Selection of Priority

In the human interface, there may be an option for selecting directory access priority. Such a feature must be used responsibly, considering DSA capacity and the relative urgency of the request. The default for priority should be set to normal. It is recommended that Urgent Priority directory accesses be reserved for tactical operations.

b. DSA Priority Processing

DSAs should be capable of servicing the priority field. However, this will depend on the queuing, processing architecture, and DIT storage mechanisms that a DSA uses. Suffice it to say that the operations in the input queues of a DSA must be serviced according to priority.

c. DAP Service Parameters

The Size Limit and Time Limit Service Control parameters should be defaulted to catch/inhibit any unexpectedly large (gigabyte) responses or dead DSAs in the chain. For example, Size Limit is defaulted to the number of objects that can be contained in 250 kilobytes.

d. DSA Performance Reporting

The DSAs shall provide performance reports which demonstrate characteristics of population, speed of access, speed of basic and filtered searches, and DIT modification/replication actions.

e. DSA Association Limits

All DSAs shall support at least 100 simultaneous associations.

f. DSA Bind Time Limits

It shall take less than ten seconds for a DSA to perform a Bind or Unbind with strong authentication with a DUA or other DSA.

g. Bogus Searches

When a search for a bogus entry is instigated (e.g., find bogus entry), the response shall be returned in less than 30 seconds, preferably ten.

h. Access Control Processing

When access controls are applied to Reads, Lists, and Searches, etc., to restrict access to identified users, they shall not increase access time by more than ten percent of the time for unrestricted access.

i. Chained Operations

When a Search is chained by a DSA (using DSP), it is a DSA performance requirement that Search requests to the other DSAs shall be initiated within ten seconds of the initial DSA access.

j. Performance Optimization Tools

It is possible that, as the allied system evolves, utilities will be developed that do scripted actions on the directory system. To assist in performance optimization of the Allied Directory System, some form of service logging and tuning tools must be used.

k. Alias/List Utilities For DIT Integrity

To assist in DIT management, alias integrity checking and clean-up facilities should be sought.

l. Replication Triggers And Consistency

When replication is used (via DISP, etc.), mechanisms must be sought that control when an update takes effect in the target DSA. This is necessary to prevent loss of data integrity in a multi-processing environment caused by the data being “overwritten” while a Search operation is also in progress.

m. Performance Logs And Reports

DUAs and DSAs shall keep transaction logs that support performance management and system planning.

322. DUA Caching Guidelines

Employing DUA caching is a matter of national policy. When it is done, the guidelines in this paragraph may be followed.

a. Store cached information in nonvolatile memory.

b. Treat cached entries and cached certificates separately for the purpose of determining the useful life of the cached information. Extend the useful cache period for the certificate, since it is a relatively static entity with its own expiration time and revocation procedures.

c. Set the time-to-live for cached information according to the type of information stored in the cache (individual or organizational), the function of the command or persons operating the system, the maximum authorized message precedence, the security classification of the information and the DUA user, and the nature of the DUA.

d. Set the time-to-live for cached entries of individual users to expire within a 15 day time period. Set the time-to-live for cached entries of organizational users to have a maximum expiration period of four days.

e. Where an organizational user and individual user share the same DUA, the expiration for the limit on the time-to-live conforms to that for the organizational user. The local management center approves time-to-live values in excess of these recommendations.

f. Capture and record, with the cached entry, the date and time that the entry was last obtained in order to determine the expiration time of the entry.

g. Upon receipt of a CRL, all components containing cached certificates compare the cached certificates against the list of revoked certificates and purge those cached certificates matching the certificates listed in the CRL.

h. Cache expiration intervals are approved in advance by the local management center. This is to avoid saturation of the directory for inappropriate short intervals. The Local Center also requests that the cache maximum time limits be raised for conditions where the directory service is unable to provide adequate service.

i. Purge a cached certificate upon the expiration date contained within the certificate.

j. Cache knowledge information of DIB distribution in DSAs, unless it violates local security guidelines. This information may be used by DUAs to gain direct access to desired information.

SECTION VI

CHAINING

323. Chaining Policy

a. All Border DSAs and DSAs in combined task forces shall be capable of supporting both chaining and referrals.

b. Either chaining or referral may be used as long as performance and security requirements are met.

c. In the service controls, Prefer Chaining shall be the favored option. However, use of Chaining Prohibited is permitted.

CHAPTER 4

DIRECTORY SECURITY POLICES AND PROCEDURES

SECTION I

SECURITY

401. Security Services

a. The security services defined within this section have been developed as countermeasures against the perceived vulnerabilities of the X.500 model. This analysis was based on X.509, Annex B. The security services defined below are considered against the three general threats of unauthorized disclosure, modification, or unavailability of information contained in the directory. The information is vulnerable when held within a DSA or when transiting elements of the directory. The aggregation of the total information shared within the allied directory may raise the level of security risk, so although individual elements of information may be of low classification, the total system may have to be considered at higher classification.

b. Not all security services will be applied to the information within the directory. For example, confidentiality of information within the directory is only considered viable when a small amount of information is at a higher classification level than the rest of the directory and the information is to be shared amongst a small number of users.

c. Many applications and services will have requirements for security. Such requirements are derived from the need to protect the information from a range of potential threats. In order to protect against threats, security services shall be provided. These services are:

- Authentication
- Access Control
- Key Management
- Confidentiality
- Labeling
- Availability
- Integrity

402. Authentication

a. Peer entity authentication is performed between DUAs and DSAs and between DSAs to provide corroboration that a user or entity in a certain instance of communication is the one claimed. ACP 133 shall support mutual authentication through the use of strong authentication. Strong authentication relies on the use of asymmetric encryption. Asymmetric encryption uses the combination of a public component and a private component to sign digitally the credentials of the user or entity authenticating itself to the system. A digital signature guarantees both the origin and the integrity of the information that is digitally signed. This binding of the public key and its holder's identification information is conveyed through an X.509 certificate that is generated by a CA. Each individual nation shall implement its own CMI to include CAs in such a manner as to ensure the trusted path for certificate management. In the case of a CTF, authentication policies and procedures are under the control of the CTF commander.

b. The CMI is an integrated relationship of CAs and all the components necessary that operate under the authority of either a superior CA or, in conjunction with bilateral agreements, with other CAs.

c. The CMI includes the process for developing Certificate Policies. A Certificate Policy is a named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements. For example, a particular Certificate Policy might indicate applicability of a type of certificate to the authentication of electronic data interchange transactions for the trading of goods within a given price range.

d. Each CA shall have a statement of the practices, the CPS, which it employs in managing certificates.

e. Each nation's CPS shall identify the procedure used to create, maintain, and revoke credentials.

f. Two-way mutual peer-to-peer strong authentication shall be supported. Strong authentication shall be used in the Allied Directory System where warranted. ACP 133 shall support attributes for Version 3 X.509 certificates and Version 2 CRLs.

g. Assurance is incumbent on the availability of public keys in a way that guarantees that the public key really belongs to a particular identity. Validation of signatures is based on the assumption that the authenticating entity has the correct public key. The link between an identity and its public key shall be guaranteed. False identities and substituted keys are serious threats to these mechanisms. Each CMI's CPS shall ensure that actions are taken to mitigate these threats.

h. Within the ACP 133 Directory system, all DSAs shall be able to process bind requests that are simply authenticated and those that are strongly authenticated, utilizing an agreed upon digital signature algorithm. DSAs shall support access control policy that prevents unauthorized disclosure or modification of information based on the level of authentication used. The DSA shall strongly authenticate itself to its communication peer (i.e., DSAs, DUAs, and management

entities) as required. The success or failure of the steps in the authentication process shall be audited and stored in the DSA audit database to facilitate compromise recovery and to enhance security of the Directory.

i. In the Allied Directory, the following additional security constraints shall be met.

(1) Prior to exchanging any information, any pair of DSAs shall strongly authenticate themselves to each other if required by security policy between the two DSAs. Additionally, the DSAs shall not permit access to any information until all access control checks have been performed and granted.

(2) Only approved cryptographic mechanisms for the DSA application and the associated processes shall be used.

(3) The DSA shall support a CMI-defined signature validation process. This process shall include validating the CA which produced the certificate used to sign the identification and authentication information (i.e., validate the certification path).

(4) If the claimed identity is not validated, the request shall be rejected and the failure audited. Additional security actions may also be initiated; for example, the DSA may lock out the user.

(5) In those environments where Rule-based Access Control (RBAC) is imposed, each entity shall exchange privilege/authorization information required for the access control decision function, when performing the strong authentication Bind operation.

(6) Once the communications partners have successfully authenticated themselves to each other, the DSA shall limit access to information stored within its DSA according to the parent (host) system security policy.

(7) The DSA shall allow access and privileges to be set only by an authorized management entity.

403. Access Control - General

a. The X.500 Directory standard defines three access control schemes: Simplified Access Control, Basic Access Control (BAC), and RBAC. However, how that information is stored within a country's directory is a national issue. The ACP 133 shall mandate that directory systems ensure that the agreed-upon access controls are maintained.

b. The access control mechanisms shall include both RBAC as well as BAC. RBAC restricts access to objects within the directory by use of predefined labels to enforce access rights to information stored within the Directory. User or end-entity authorization information may be exchanged through extensions to the Version 3 X.509 certificates. ACI about the target (data within the DIB) shall be conveyed through the use of sensitivity labels. The format and processes associated with the privilege/authorization information are defined within each CMI's

CPS. The format and processes associated with security labels are defined in an Annex of ACP 120.

c. Within the Allied Directory Service there is a requirement to hold information at different levels of protective marking, and therefore, it is necessary to have a method by which the confidentiality of the information can be maintained without disclosure to unauthorized access. In addition, there may be occasions where information will be stored in a Directory that is of a higher classification than that which the DSA normally supports, or is of a sensitive nature and requires separation from disclosure to system administrators and other authorized users. This requirement shall be supported by one of the following mechanisms, in accordance with security policy:

- encryption of the stored information to protect its content from unauthorized disclosure
- access control mechanisms to protect the stored information from unauthorized access
- the use of both services

404. Basic Access Control

a. BAC is based on a relatively simple concept: either a list of users and the permissions to which they are entitled, or a list of protected items and the permissions necessary to access them, is held within the directory. This information is contained within ACI items. ACI items can be held within a number of parts of the directory depending on their intended usage and sphere of influence.

b. Each ACI item consists of four parts.

(1) Identification tag is used to name a particular ACI item.

(2) Precedence level is a number which determines the order in which ACI items should be considered. An item with a higher precedence will overrule an item with a lower precedence.

(3) Authentication level is the level to which the user must be authenticated. This can be no authentication, simple authentication, strong authentication, or by some external method.

(4) Either Item first permissions, which lists a set of protected items, and the set of users, all potentially with varying permissions, or User first permissions which lists a set of users and the protected items, all potentially with varying permissions that the users may or may not access is the fourth part.

405. Rule-based Access Control

a. Within ACP 133 and the civil standards arena, a requirement for additional information to be included in determining whether access can be granted or denied to an object has been identified. This is defined as RBAC, and requires administratively imposed access control policies to be applied to the contents of the directory.

b. RBAC uses security labels that can be attached (by securely binding the label to the information using a digital signature) to attribute values stored within the directory. The security label of an attribute shall be bound to the attribute value using a digital signature. This label can then be used to determine whether a user may access protected information. RBAC can be used alone, or in conjunction with BAC. Refer to clause 17.4.3 in ITU-T Rec. X.501 (1997) | ISO/IEC 9594-2: 1997.

c. RBAC adds the following constraints on the access control decision.

(1) DiscloseOnError is not supported under RBAC, and hence if Read access is denied, then the operation acts as if the entry does not exist.

(2) RBAC affects operations on reading attribute values (e.g., Read and Search) in that the attribute value is not visible if access is not authorized (operation is carried out as though the attribute value is not present). It does not currently affect operations on entries as a whole which do not impact on existing attribute values (e.g., Add Entry).

(3) RBAC operations which involve removing an attribute value (e.g., Remove Entry, Modify Entry, and Remove Attribute) fail if the access is not authorized.

(4) If access to all attributes of an entry is denied under RBAC, access is denied to that entry for all operations.

d. An error code is returned from an operation or the attribute value, attribute type, or entry is omitted from the operation result if:

- the label for the attribute value denies access, then the attribute value is hidden
- the labels for attribute values of a given type deny access, the existence of the attribute is hidden (If access is denied to all attribute values of a type, then access is denied to that type.)
- the labels for attribute values of a given entry deny access, the existence of the entry is hidden (If access is denied to all attribute values of an entry, then access is denied to that entry.)

e. To enforce RBAC, initiator-bound access control information (clearance information) needs to be provided to enable a comparison to be made with the target's security label. Clause 17.5 of ITU-T Rec. X.501(1997) | ISO/IEC 9594-2: 1997 identifies the syntactic representation

for the clearance attribute. There are at least two methods to convey this information with integrity.

(1) The user's clearance can be bound to the user's DN and the public key used to authenticate that DN with a public key certificate extension.

(2) The user's clearance can be bound to the user's DN and to the user's X.509 certificate using an attribute certificate.

f. If the first method is chosen, and the authority verifying the public key information of a user may or may not be the same authority that is responsible for issuing and verifying a user's clearance, the clearance must be supplied to the CA in a trusted manner.

g. Each CMI's CPS shall include the procedures required to validate each end-entity's identity and privilege/authorizations.

h. The security labels will be based on a hierarchical set: UNCLASSIFIED, RESTRICTED, CONFIDENTIAL, SECRET and TOP SECRET, that can be compared to the clearance of the requester based on a corresponding set of hierarchical class values. These hierarchical classifications form the "base set" for the RBAC scheme and will be extended to address privilege information conveyed in a security category and/or privilege marking.

i. In resolving permissions, the DSA shall first obtain the clearance of the user from a trusted source. This information shall be conveyed during the authentication process. When obtained, the contents of the security label is checked against the user's clearance. RBAC does not define what type of subsequent operations may be performed, e.g., modify, remove etc.

406. Access Control Decision Function

a. In the event that RBAC has been implemented, additional steps in the access control transforms must occur. First, the hierarchical clearance of the user must dominate the hierarchical classification of the label. Second, if additional categories have been applied to the security label, there must be a comparison function between the security categories component of both the data label and the user clearances. If RBAC succeeds and there are no additional RBAC restrictions imposed, the user is granted access. The security policy rules defining the relationship between the end-entity's privilege/authorization set and the security label shall be provided by each nation's appropriate authority.

b. The Access Control Decision Function (ACDF) specifies how ACI items shall be processed in order to determine whether access should be granted for a particular operation.

c. Figure 4-1 and Figure 4-2 are based on the ISO/IEC 10181-3 Security Framework in Open Systems standard (Part 3 - access controls), but have been adapted to fit the BAC model described in the X.500 standard. The ACDF makes the decision as to whether to grant or deny access to the requested object(s) by applying pre-defined access control policy rules to an access request.

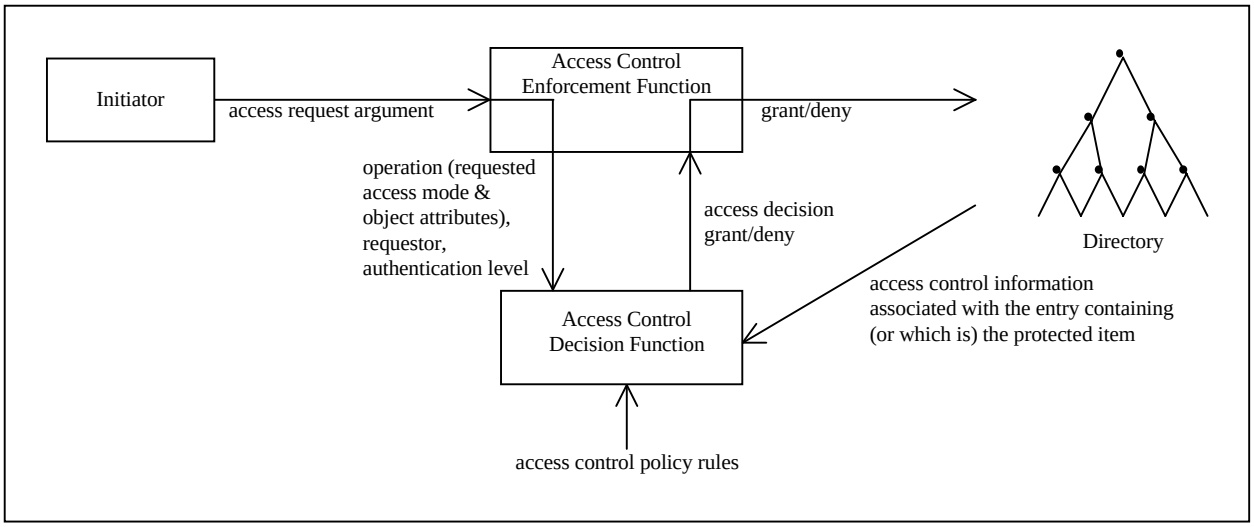

Figure 4-1
Diagram of ACDF Required for Basic Access Control

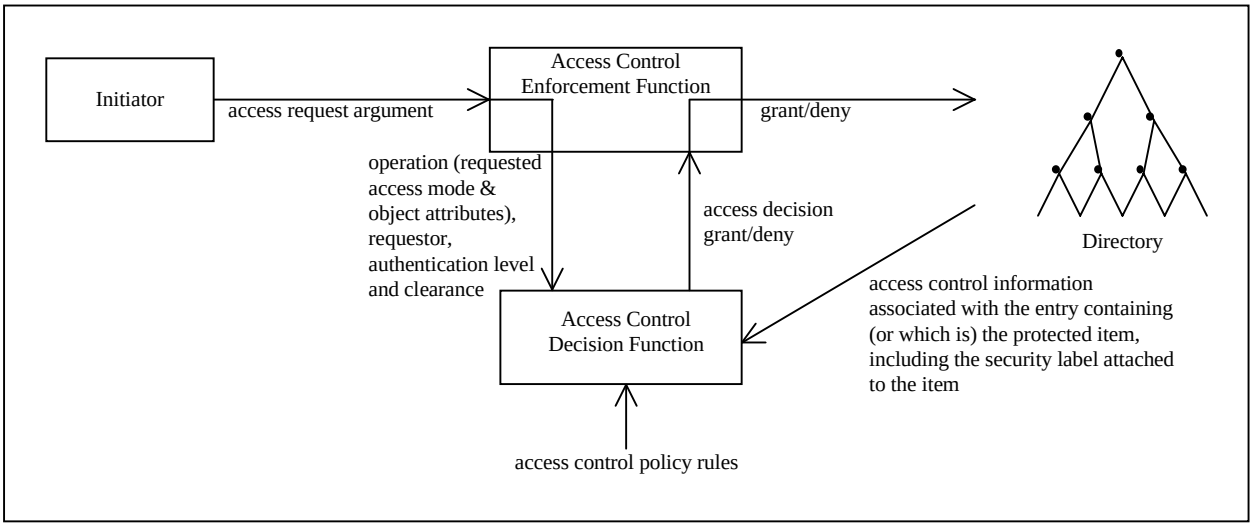

Figure 4-2
Diagram of ACDF Required for Rule-based and Basic Access Control

d. If RBAC is being used in conjunction with BAC, then RBAC should always take precedence over the BAC. Therefore, if RBAC scheme rules do not allow access to a requested operation, then the operation will be denied independently of whether access would have been granted under the BAC scheme. Only if the RBAC scheme rules allow access to a requested operation will the ACDF for BAC be executed to determine if access should be granted.

e. A policy identifier shall be used to identify under which security policy the clearance and security labeling are being enforced.

f. The security policy is represented by an object identifier that indicates the security policy the subject supports. Each security policy registered shall have documentation that indicates the values of classifications and privilege/authorization sets valid within the context of that security policy.

407. Key Management

a. Common cryptographic algorithms and their intended usage need to be supported. National CPS will define acceptable cryptographic algorithms and required usages.

b. In the event that a DSA's signature or confidentiality keys are compromised, immediate notification to the Security Authority shall occur.

408. Confidentiality

a. In some situations, the Allied Directory may not give sufficient assurance that data is kept confidential in storage, regardless of access controls. Confidentiality of attributes in storage is provided through use of:

- a template for the definition of attributes which are protected by a security transformation which provides confidentiality (Refer to Clause 18.2.2 of ITU-T X.501 (1997) | ISO/IEC 9594-2: 1997.)

- an attribute for distributing keys to those who need to decrypt attributes using the identified key. The key being distributed is protected by encrypting the key value with the public key of each authorized reader of the attribute. (Refer to Clause 18.2.3 of ITU-T X.501 (1997) | ISO/IEC 9594-2: 1997.)

b. Note: Other mechanisms can be used to distribute the keys required to protect attributes defined using the Encrypted Attribute Value template.

409. Labeling

a. General

A common policy on labeling and clearance is the basis for labeling in the Allied Directory. The format and processes associated with security labels are defined in an Annex of ACP 120. Labeling and clearance information implemented in the Allied Directory Services shall support access control in the shared information environments.

b. Security Classification

(1) The following security classifications are valid:

- UNCLASSIFIED
- RESTRICTED
- CONFIDENTIAL
- SECRET
- TOP SECRET

(2) These classifications are hierarchical and are listed in ascending order, that is, Restricted is a higher classification than UNCLASSIFIED.

(3) Within subject Clearances issued to end-entities, the following classifications are valid:

- UNCLASSIFIED
- RESTRICTED
- CONFIDENTIAL
- SECRET
- TOP SECRET

(4) These clearances are listed in hierarchical order with Top Secret dominating Secret and so on. A Top Secret clearance allows access to all other information unless other restrictions apply. The rules governing the population of the clearance attribute are defined in each CMI's certificate policy.

c. Categories

(1) Categories may be divided into multiple groups. At a minimum, the following types shall be supported: Restrictive, Permissive, and User-Defined.

(2) A Restrictive Category requires that all values present in the security label shall be present in the authorizations conveyed in the clearance.

(3) Permissive Categories require that at least one value present in the security label shall be present in the authorizations conveyed in the clearance. This is applicable when indicating the capability to constrain access by nationality, for example, Release To or Eyes Only.

(4) User-Defined Categories shall be identified when implemented across international boundaries.

(5) An ACDF matches the user or end-entity's clearances and the attribute security label to determine if the user or end-entity is allowed to access the attribute value. The permissive categories are checked by access control functions to ensure that if any one of the bits in the extension match the bits in the security label, the attribute can be accessed. The restrictive categories are used by access control functions to ensure that all bits in the certificate extension match all the bits in the label prior to granting access. The user-defined categories shall process in accordance with the registered procedures.

d. Privacy Markings

Privacy markings are text handling instructions and warnings. They provide no support for access control decisions.

e. Policy Identifiers

(1) The set of the categories and classifications and their semantic interpretation is defined in context of the policy identifier.

(2) Multiple security policies will exist and need to be supported. Equivalency mapping will be identified through the cross certification processes.

410. Availability

Availability of the data in the Allied Directory System shall be ensured through robust replication and disaster recovery practices.

411. Integrity

a. Data integrity provides proof of the integrity of the information, either in storage or while in communications channels. The mechanism involves encipherment of a compressed string of the relevant data to be stored or transferred. This will be a function of the digital signature mechanisms using an asymmetric scheme.

b. In the event integrity is required on information stored in the directory, the information shall be signed. The user who requires validation of the integrity of that information shall validate the signature to ensure no unauthorized modifications have occurred. The definition of an attribute type to hold a digital signature, along with associated control information, which provides integrity of a whole entry or all values of selected attribute types is found in clause 18.1.2 of ITU-T X.501 (1997) | ISO/IEC 9594-2: 1997.

c. The Allied Directory shall support integrity on a single attribute value. The definition of the Attribute Value Integrity Information Context is found in Clause 18.1.3 of ITU-T X.501 (1997) | ISO/IEC 9594-2: 1997.

d. The Allied Directory shall be capable of supporting signed operations on all operation requests received, as well as generate signed responses to those arguments. This shall include error responses. The integrity protection required shall be negotiated and agreed-upon when establishing connectivity. For those combined task force environments that cannot support the required protection, then the information may be returned unprotected. The decision to utilize the information is up to the policies of the task force commander.

SECTION II

ACCOUNTABILITY/AUDITING

412. Data Protection

Any of the information that is stored within a Security Management Information Base (SMIB) shall be protected against manipulation or destruction by unauthorized users or end entities. Changing any of the thresholds associated with collection of audit information shall be made available only to those authorized audit management entities. When information from one domain is replicated into another domain, the agreement to shadow shall contain details on how archive of and access to audit data will be supported.

CHAPTER 5

DIRECTORY MANAGEMENT POLICIES AND PROCEDURES

501. Scope

a. The policies defined in this document for management are applicable to the directory system component level of the Allied Directory System. Additional requirements such as help desks and operations relating to the higher level system issues of the Allied Directory System will be covered in related documents.

b. There are three operational areas of management to consider.

(1) Management of each nation's domain shall be done at the national level and is out of the scope of this document.

(2) Management of a combined domain shall be done in accordance with this ACP and under the control of the commander of the CTF.

(3) Management of the international domain, such as the management of Border DSAs shall be performed as defined in this ACP and other Allied documents.

502. Mandated Functionality

For the purposes of insuring a base level of management functionality within the Allied Directory System components, the following features and functions are mandated.

a. All DSAs and DUAs shall be capable of extending the schema to include new object classes and attributes and, optionally, new syntaxes without recourse to software rework.

b. All DSAs shall be able to have ACI and other subentry information configurable.

c. All DSAs shall be able to have their replication agreements configurable.

d. All DSAs shall support logging facilities as defined in paragraph 504.

e. All DSAs shall support, as a minimum, the X.500 Directory Monitoring Management Information Base (MIB) defined in RFC 1567, or equivalent.

f. All DSAs shall support the generation of events or alarms and log entries that reflect error conditions such as resource problems, protocol failures, or system security violations. Sample alarms include:

- security violations (unable to authenticate DUA-DSA or DSA-DSA)
- connection failure

- resource limits encountered
- process error

g. All DSAs shall provide a management console interface that will permit local and remote management. Remote management facilities shall be applied with some authorization and protection mechanism.

503. Desirable Additional Functionality

The following additional features and functions are desirable.

a. DUAs should be configurable by a system administrator to control the services that are permitted to the DUA user. Note that the Allies intend to control the extent of DAP operations by DUAs by configuring the DUA and by access control information in the DSA.

b. Management interfaces of Directory components should apply standard protocols such as DAP, CMIP and/or SNMP.

c. Management logs and log controls should reflect the functionality defined in ITU-T Rec. X.735 | ISO/IEC 10164-6.

d. Management facilities provided with directory components should relate to directory domains, i.e., multi-DSA systems.

504. Event Logs

a. DSAs shall provide for the logging of all operations with various levels of detail. Log control mechanisms shall provide configuration or functions for:

- controlling the size of log
- action taken when a file is full, e.g., overwrite the log or create a new file
- deleting or archiving the log
- controlling logging levels
- starting and stopping logging

b. Log entries shall provide:

- event time
- event type
- operation type (e.g., List, Modify, Modify DN)

- originator's DN
- target object
- outcome of request or response, i.e., success, failure, error, etc.
- major parameters:
  - service controls
  - filter used
  - security parameters
  - entryInformationSelection

c. DSAs shall support recording the following errors:

- errors defined in clause 12 of X.511, such as, nameError, updateError, attributeError, securityError, abandoned, abandonFailed
- errors defined in clause 12 of X.525, such as, shadowError. Sample problems are unsupportedStrategy and inactiveAgreement.
- errors defined in clause 24 of X.501, such as, operationalBindingError. Sample problems are invalidAgreement and notAllowedForRole.
- errors defined in clauses 11 - 13 of X.518, such as, dsaReferral

505. Service Level Agreements

A SLA is the formal agreement to be used between Allies for the operation of an ACP 133-compliant directory. Such agreements shall be established on a bilateral basis between Allies and shall address the quality, quantity, and, where appropriate, the cost of the directory service to be established. An SLA shall include sufficient definitions and measures of performance to cover the type of service, the quantity and quality of the service required, and any time-scale targets. In principle, SLAs should be written to a common format and, to this end, a suggested outline is given in Annex F.

ANNEX A

REFERENCE DOCUMENTS

1. International

a. ACP 100, Allied Call Sign and Address Group System Instructions and Assignments

b. ACP 117, *Allied Routing Indicator Book*

c. ACP 120, "Common Security Protocol (CSP)", final draft

d. ACP 123, *Common Messaging Strategy and Procedures*, November, 1994

e. ACP 127, *Communications Instructions - Tape Relay Procedures*

f. "CMI CONOPS", draft

g. CCITT Recommendation E.123 (1988), *Notation for National and International Telephone numbers*

h. CCITT Recommendation F.1 (1992), *Operational provisions for the international public telegram service*

i. CCITT Recommendation F.200 (1992), *Teletex service*

j. CCITT Recommendation F.31 (1988), *Telegram Retransmission System*

k. CCITT Recommendation T.62 (1993), *Control procedures for teletex and Group 4 facsimile services*

l. CCITT Recommendation X.200 (1988), *Reference Model of Open Systems Interconnection for CCITT Applications*

m. CCITT Recommendation X.735 (1992) | ISO/IEC 10164-6:1992, *Information technology - Open Systems Interconnection - Systems Management: Log control function*

n. CCITT Recommendation X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*

o. ISO 3166-1: 1997, *Codes for the representation of names of countries and their subdivsions - part 1: Country codes*

p. ISO 7498-2: 1987, *Information processing systems - Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture*

q. ISO/IEC ISP 15125-0, "Information Technology - International Standardized Profile - Common upper layer requirements - For the Directory", draft 1, 30 May 1996

r. ISO/IEC ISP 15125-1, “Information Technology - International Standardized Profiles ADY11 - The Directory - DUA support of Directory Access Protocol”, draft 8, 19 June 1998

s. ISO/IEC ISP 15125-2, “Information Technology - International Standardized Profiles ADY12 - The Directory - DUA support of Distributed Operations”, draft 6, 19 June 1998

t. ISO/IEC ISP 15125-3, “Information Technology - International Standardized Profiles ADY21- The Directory - DSA support of Directory Access Protocol”, draft 5, 19 June 1998

u. ISO/IEC ISP 15125-4, “Information Technology - International Standardized Profiles ADY22 - The Directory - DSA support of Distributed Operations”, final draft, 20 January 1997

v. ISO/IEC ISP 15125-5, “Information Technology - International Standardized Profiles ADY41 - The Directory - DUA Authentication as DAP initiator”, draft 10, 19 June 1998

w. ISO/IEC ISP 15125-6, “Information Technology - International Standardized Profiles ADY42 - The Directory - DSA Authentication as DAP responder”, draft 8, 19 June 1998

x. ISO/IEC ISP 15125-7, “Information Technology - International Standardized Profiles ADY43 - The Directory - DSA Authentication for DSP”, draft 8, 22 July 1996

y. ISO/IEC ISP 15125-9, “Information Technology - International Standardized Profiles ADY45 - The Directory - DSA Basic Access Control”, draft 6, 24 July 1998

z. ISO/IEC ISP 15125-10, “Information Technology - International Standardized Profiles ADY51 - The Directory - Shadowing using ROSE”, draft 5, 12 July 1996

aa. ISO/IEC ISP 15125-12, “Information Technology - International Standardized Profiles ADY53 - The Directory - Shadowing subset”, draft 5, 12 July 1996

bb. ISO/IEC ISP 15125-13, “Information Technology - International Standardized Profiles ADY61 - The Directory - Administrative areas”, draft 4, 26 June 1998

cc. ISO/IEC ISP 15125-14, “Information Technology - International Standardized Profiles ADY62 - The Directory - Establishment and utilization of shadowing agreements”, draft 1, 17 Jan. 1997

dd. ISO/IEC ISP 15125-15, “Information Technology - International Standardized Profiles ADY63 - Schema administration and publication”, draft 3, 30 November, 1998

ee. ISO/IEC ISP 15125-16, “Information Technology - International Standardized Profiles ADY71 - The Directory - Shadowing Operational Binding”, draft 1, 30 July 1996

ff. ISO/IEC ISP 15125-17, “Information Technology - International Standardized Profiles ADY72 - The Directory - Hierarchical Operational Binding”, Internet draft, Dec. 1997

gg. ISO/IEC ISP 15126-1, “Information Technology - International Standardized Profiles FDY11 - The Directory - Common Directory Use”, draft 7, 17 July 1996

hh. ISO/IEC ISP 15126-2, "Information Technology - International Standardized Profiles FDY12 - The Directory - Directory System Schema", draft 5, 17 July 1996

ii. ISO/IEC TR 10000-1: 1995, *Information Technology - Framework and taxonomy of International Standardized Profiles - Part 1: Framework*

jj. ISO/IEC TR 10000-2: 1995, *Information Technology - Framework and taxonomy of International Standardized Profiles - Part 2: Principles and taxonomy for OSI profiles*

kk. ITU-T Recommendation X.402 (1995) | ISO/IEC 10021-2: 1996 *Information technology - Message Handling Systems (MHS) - Overall Architecture*

ll. ITU-T Recommendation X.500 (1993) | ISO/IEC 9594-1: 1995, *Information technology - Open Systems Interconnection - The Directory: Overview of concepts, models and services*

mm. ITU-T Recommendation X.501 (1993) | ISO/IEC 9594-2: 1995, *Information technology - Open Systems Interconnection - The Directory: Models*

nn. ITU-T Recommendation X.501 (1997) | ISO/IEC 9594-2: 1997, "Information technology - Open Systems Interconnection - The Directory: Models"

oo. ITU-T Recommendation X.509 (1993) | ISO/IEC 9594-8: 1995, *Information technology - Open Systems Interconnection - The Directory: Authentication framework*

pp. ITU-T Recommendation X.509 (1997) | ISO/IEC 9594-8: 1997, "Information technology - Open Systems Interconnection - The Directory: Authentication framework"

qq. ITU-T Recommendation X.511 (1993) | ISO/IEC 9594-3: 1995, *Information technology - Open Systems Interconnection - The Directory: Abstract service definition*

rr. ITU-T Recommendation X.518 (1993) | ISO/IEC 9594-4: 1995, *Information technology - Open Systems Interconnection - The Directory: Procedures for distributed operation*

ss. ITU-T Recommendation X.519 (1993) | ISO/IEC 9594-5: 1995, *Information technology - Open Systems Interconnection - The Directory: Protocol specifications*

tt. ITU-T Recommendation X.520 (1993) | ISO/IEC 9594-6: 1995, *Information technology - Open Systems Interconnection - The Directory: Selected attribute types*

uu. ITU-T Recommendation X.520 (1997) | ISO/IEC 9594-6: 1997, "Information technology - Open Systems Interconnection - The Directory: Selected attribute types"

vv. ITU-T Recommendation X.521 (1993) | ISO/IEC 9594-7: 1995, *Information technology - Open Systems Interconnection - The Directory: Selected object classes*

ww.ITU-T Recommendation X.521 (1997) | ISO/IEC 9594-7: 1997, "Information technology - Open Systems Interconnection - The Directory: Selected object classes"

xx. ITU-T Recommendation X.525 (1993) | ISO/IEC 9594-9: 1995, *Information technology - Open Systems Interconnection - The Directory: Replication*

yy. ITU-T Recommendation X.530 (1997) | ISO/IEC 9594-10: 1997, "Information Technology - Open Systems Interconnection - The Directory: Use of Systems Management for Administration of the Directory"

zz. ITU-T Recommendation X.583(1997) | ISO/IEC 13248-1:1998, *Information Technology -- Open Systems Interconnection -- Directory Access Protocol: Protocol Implementation Conformance Statement (PICS) Proforma*

aaa.ITU-T Recommendation X.584(1997) | ISO/IEC 13248-2:1998, *Information Technology -- Open Systems Interconnection -- Directory System Protocol: Protocol Implementation Conformance Statement (PICS) Proforma*

bbb.ITU-T Recommendation X.585(1997) | ISO/IEC 13248-3:1998, *Information Technology -- Open Systems Interconnection -- Directory Operational Binding Management Protocol: Protocol Implementation Conformance Statement (PICS) Proforma*

ccc.ITU-T Recommendation X.586(1997) | ISO/IEC 13248-4:1998, *Information Technology -- Open Systems Interconnection -- Directory Information Shadowing Protocol: Protocol Implementation Conformance Statement (PICS) Proforma*

ddd.ITU-T Recommendation X.680 (1994) | ISO/IEC 8824-1: 1994, *Information technology - Abstract Syntax Notation One (ASN.1): Specification of basic notation*

eee.ITU-T Recommendation X.681 (1994) | ISO/IEC 8824-2: 1994, *Information technology - Abstract Syntax Notation One (ASN.1): Information object specification*

fff. ITU-T Recommendation X.682 (1994) | ISO/IEC 8824-3: 1994, *Information technology - Abstract Syntax Notation One (ASN.1): Constraint specification*

ggg.ITU-T Recommendation X.683 (1994) | ISO/IEC 8824-4: 1994, *Information technology - Abstract Syntax Notation One (ASN.1): Parameterization of ASN.1 specifications*

hhh.ITU-T Recommendation X.812 (1995) | ISO/IEC 10181-3: 1996, *Information technology - Open Systems Interconnection - Security Frameworks in Open Systems - Access control framework*

iii. ITU-T Recommendation X.880 (1994) | ISO/IEC 13712-1: 1994, *Information technology - Remote Operations: Concepts, model and notation*

2. General

a. Barker, P. and Kille, S., November 1991, "The COSINE and Internet X.500 Schema", RFC 1274

b. Boeyen, S., Howes, T., and Richard, P., September 1998, "Internet X.509 Public Key Infrastructure - LDAPv2 Schema"

c. Mansfield, G. and Kille, S., January 1994, "X.500 Directory Monitoring MIB," RFC 1567

d. Smith, Mark, 17 November 1998, "Internet-Draft: Definition of the inetOrgPerson LDAP Object Class"

3. National

a. Joint Chiefs of Staff, March 1983, Automatic Digital Network (AUTODIN) Operating Procedures, JANAP128(I)

4. Corrigenda to the X.500 Series of Recommendations | ISO/IEC 9594 not included in ISPs

5. Amendments to to the X.500 Series of Recommendations | ISO/IEC 9594 not included in ISPs

a. Final proposed Draft Amendments to Support the UTF8 Encoding of the ISO/IEC 10646 Character Set," January 1998.

b. ISO/IEC JTC 1 SC6 N11013, DAM to ISO/IEC Parts 7 and 8, The Directory - Amendments on Certificate Extensions, September 1998

ANNEX B

SCHEMA

TABLE OF CONTENTS

SECTION I

CONCEPTS

SECTION II

COMMON STRUCTURAL OBJECT CLASSES AND NAME FORMS

SECTION IV

APPLYING CONTENT RULES IN THE COMMON CONTENT

SECTION XII

ACP 133 DATA TYPES

List of Figures

List of Tables

SECTION I

CONCEPTS

1. General

a. The ACP 133 schema is based to the extent possible on civilian standards, in particular, ITU-T Rec. X.402 (1995), ITU-T Rec. X.509 (1993), ITU-T Rec. X.520 (1993), and ITU-T Rec. X.521 (1993) plus the 1997 operational security and certificate extensions to ITU-T Rec. X.509 , ITU-T Rec. X.520 and ITU-T Rec. X.521. Several object classes have been introduced that are included in the Certificate Extensions DAM 1 to ISO/IEC 9594 Parts 7 & 8 (i.e., X.521 & X.509) that is being applied to the 1997 Directory Standards. In the Allied Directory System, all of the object classes, attributes, matching rules, and name forms defined in X.501, X.509, X.520, X.521, X.402, and the DAM shall be implemented.

b. This ACP defines a “common content” which is the schema that must be implemented for the Allied Directory System. Each directory entry in the Allied Directory System is defined by a structural object class and, potentially, a content rule. The content rule includes the structural object class, allowed auxiliary object classes, and additional attributes.

c. Examples of content rules are given in Section IV of this annex. Inclusion of auxiliary object classes and additional attributes depends on the application, as specified in Chapter 3. For example, an entry for an organizational unit which does secure ACP 123 messaging would include the mhs-user and securePkiUser auxiliary object classes. An organizational unit which is used for DIT navigational purposes would not populate those classes.

d. Each country may construct a content rule based on a structural object class and may include additional auxiliary object classes and more attributes as long as at least the Common Content is supported.

e. Besides the Common Content, this annex also contains definitions of generally useful object classes and attributes.

SECTION II

COMMON STRUCTURAL OBJECT CLASSES AND NAME FORMS

2. Common Structural Object Classes

The Allied Common Content includes standard structural object classes and structural object classes defined in this ACP. The Allied Directory System entries defined using these structural object classes are described in Section IV of this annex.

3. Directory Standard Structural Object Classes

a. Base Object Classes

Although all of the directory standard structural object classes shall be supported for the Allied Directory System, the Common Content uses only the following standard classes as the structural object classes of Allied Directory Entries:

- applicationEntity
- applicationProcess
- country
- cRLDistributionPoint
- device
- dSA
- groupOfNames
- locality
- organization
- organizationalPerson
- organizationalRole
- organizationalUnit

b. Superclasses

Each of these standard classes is used in the Common Content as a superclass in the definition of a standard structural object class, as described below, or of a structural object class defined in this ACP:

- alias
- applicationEntity
- mhs-message-transfer-agent
- person
- pkiUser

- strongAuthenticationUser
- top

c. Other Standard Structural Object Classes

There are several other standard structural object classes that are included in the Common Content, but which are not used to meet Allied Directory requirements. These structural object classes are:

- groupOfUniqueNames
- residentialPerson

d. Directory Standard Object Class Descriptions

The rest of this paragraph describes the directory standard structural object classes that are used as base classes in directory entries in the Common Content. Descriptions are not included for the object classes that are used solely as superclasses (e.g., person) in the Common Content.

e. applicationEntity

The applicationEntity object class is used to define directory entries representing application entities. An application entity consists of those aspects of an application process pertinent to communications. If an application entity is represented as a Directory object distinct from an application process, the commonName attribute is used to carry the value of the application entity qualifier. Table B-1 shows the composition of the applicationEntity object class. This object class is the base class for Application Entity Ed. A and Certification Authority Ed. B (see paragraph 12 g.) type directory entries and is the superclass of the base class for DSA Ed. A, MHS Message Store Ed. A, MHS Message Transfer Agent Ed. A, MHS User Agent, and MLA Ed. A type directory entries.

Table B-1
applicationEntity Object Class

Attribute	m/o
X.520: commonName	m
X.520: description	o
X.520: localityName	o
X.520: organizationalUnitName	o
X.520: organizationName	o
X.520: presentationAddress	m
X.520: seeAlso	o
X.520: supportedApplicationContext	o

f. applicationProcess

The applicationProcess object class is used to define directory entries representing application processes. An application process is an element within a computer system which performs the information processing for a particular application. Table B-2 shows the composition of the applicationProcess object class. This object class is the base class for Application Process type directory entries.

Table B-2
applicationProcess Object Class

Attribute	m/o
X.520: commonName	m
X.520: description	o
X.520: localityName	o
X.520: organizationalUnitName	o
X.520: seeAlso	o

g. country

The country object class is used to define nation directory entries. Table B-3 shows the composition of the country object class. This object class is the base class for Country type directory entries.

Table B-3
country Object Class

Attribute	m/o
X.520: countryName	m
X.520: description	o
X.520: searchGuide	o

h. cRLDistributionPoint

The cRLDistributionPoint object class is used in defining directory entries for objects which act as CRL Distribution Points as defined in ITU-T Rec. X.521 | ISO/IEC 9594-7. Table

B-4 shows the composition of the cRLDistributionPoint object class. This object class is the base class for CRL Distribution Point type directory entries.

Table B-4
cRLDistributionPoint Object Class

Attribute	m/o
X.509: authorityRevocationList	o
X.509: certificateRevocationList	o
X.520: commonName	m
X.509-1997: deltaRevocationList	o

i. device

The device object class is used to define entries representing devices. A device is a physical unit which can communicate, such as a modem, disk drive, etc. Table B-5 shows the composition of the device object class. This object class is the base class for Device Ed. A type directory entries.

Table B-5
device Object Class

Attribute	m/o
X.520: commonName	m
X.520: description	o
X.520: localityName	o*
X.520: organizationalUnitName	o
X.520: organizationName	o
X.520: owner	o*
X.520: seeAlso	o
X.520: serialNumber	o*

* At least one of localityName, serialNumber, owner, should be included. The choice is dependent on device type.

j. dSA

The dSA object class is used to define directory entries representing application entities that implement the X.500 DSA functionality. A DSA is as defined in ITU-T Rec. X.501

| ISO/IEC 9594-2. Table B-6 shows the composition of the dSA object class. This object class is the base class for DSA Ed. A type directory entries.

Table B-6
dSA Object Class

Attribute	m/o
X.520: commonName*	m
X.520: description*	o
X.520: knowledgeInformation	o
X.520: localityName*	o
X.520: organizationalUnitName*	o
X.520: organizationName*	o
X.520: presentationAddress*	m
X.520: seeAlso*	o
X.520: supportedApplicationContext*	o

* from applicationEntity (superclass)

k. groupOfNames

The groupOfNames object class is used to define directory entries representing an unordered set of names which represent individual objects or other groups of names. The membership of a group is static, i.e., it is explicitly modified by administrative action, rather than dynamically determined each time the group is referred to. The membership of a group can be reduced to a set of individual object's names by replacing each group with its membership. This process would be carried out recursively until all constituent group names have been eliminated, and only the names of individual objects remain. Table B-7 shows the composition of the groupOfNames object class. This object class is the base class for Group of Names type directory entries.

Table B-7
groupOfNames Object Class

Attribute	m/o
X.520: businessCategory	o
X.520: commonName	m
X.520: description	o
X.520: member	m
X.520: organizationalUnitName	o
X.520: organizationName	o
X.520: owner	o
X.520: seeAlso	o

l. groupOfUniqueNames

The groupOfUniqueNames object class is not used for Allied Directory entries, but is described in X.521.

m. locality

The locality object class is used to define directory entries that represent places. Table B-8 shows the composition of the locality object class. This object class is the base class for Locality type directory entries.

Table B-8
locality Object Class

Attribute	m/o
X.520: description	o
X.520: localityName	o*
X.520: searchGuide	o
X.520: seeAlso	o
X.520: stateOrProvinceName	o*
X.520: streetAddress	o

* At least one of localityName or stateOrProvinceName must be present.

n. organization

The organization object class is used to define directory entries that represent organizations. Table B-9 shows the composition of the organization object class. This object class is the base class for Organization Ed. B and Certification Authority Ed. B (see paragraph 12 g in this annex.) type directory entries.

Table B-9
organization Object Class

Attribute	m/o
X.520: businessCategory	o
X.520: description	o
X.520: destinationIndicator	o
X.520: facsimileTelephoneNumber	o
X.520: internationalISDNNumber	o
X.520: localityName	o
X.520: organizationName	m
X.520: physicalDeliveryOfficeName	o
X.520: postalAddress	o
X.520: postalCode	o
X.520: postOfficeBox	o
X.520: preferredDeliveryMethod	o
X.520: registeredAddress	o
X.520: searchGuide	o
X.520: seeAlso	o
X.520: stateOrProvinceName	o
X.520: streetAddress	o
X.520: telephoneNumber	o
X.520: teletexTerminalIdentifier	o
X.520: telexNumber	o
X.509: userPassword	o
X.520: x121Address	o

o. organizationalPerson

The organizationalPerson object class is used to define directory entries representing people employed by, or in some other important way associated with, an organization. Table B-10 shows the composition of the organizationalPerson object class. This object class is the base class for Organizational Person Ed. B type directory entries.

Table B-10
organizationalPerson Object Class

Attribute	m/o
X.520: commonName*	m
X.520: description*	o
X.520: destinationIndicator	o
X.520: facsimileTelephoneNumber	o
X.520: internationalISDNNumber	o
X.520: localityName	o
X.520: organizationalUnitName	o
X.520: physicalDeliveryOfficeName	o
X.520: postalAddress	o
X.520: postalCode	o
X.520: postOfficeBox	o
X.520: preferredDeliveryMethod	o
X.520: registeredAddress	o
X.520: seeAlso*	o
X.520: stateOrProvinceName	o
X.520: streetAddress	o
X.520: surname*	m
X.520: telephoneNumber*	o
X.520: teletexTerminalIdentifier	o
X.520: telexNumber	o
X.520: title	o
X.509: userPassword*	o
X.520: x121Address	o

* from person (superclass)

p. organizationalRole

The organizationalRole object class is used to define directory entries representing positions or roles within an organization. An organizational role is normally considered to be filled by a particular organizational person. Over its lifetime, however, an organizational role may be filled by a number of different organizational persons in succession. In general, an organizational role may be filled by a person or a non-human entity. Table B-11 shows the composition of the organizationalRole object class. This object class is the base class for Organizational Role Ed. B, Release Authority Role Ed. B, and Certification Authority Ed. B (see paragraph 12 g) type directory entries.

Table B-11
organizationalRole Object Class

Attribute	m/o
X.520: commonName	m
X.520: description	o
X.520: destinationIndicator	o
X.520: facsimileTelephoneNumber	o
X.520: internationalISDNNumber	o
X.520: localityName	o
X.520: organizationalUnitName	o
X.520: physicalDeliveryOfficeName	o
X.520: postalAddress	o
X.520: postalCode	o
X.520: postOfficeBox	o
X.520: preferredDeliveryMethod	o
X.520: registeredAddress	o
X.520: roleOccupant	o
X.520: seeAlso	o
X.520: stateOrProvinceName	o
X.520: streetAddress	o
X.520: telephoneNumber	o
X.520: teletexTerminalIdentifier	o
X.520: telexNumber	o
X.520: x121Address	o

q. organizationalUnit

The organizationalUnit object class is used to define directory entries representing subdivisions of organizations. Table B-12 shows the composition of the organizationalUnit object class. This object class is the base class for Organizational Unit Ed. B and Certification Authority Ed. B (see paragraph 12 g.) type directory entries.

Table B-12
organizationalUnit Object Class

Attribute	m/o
X.520: businessCategory	o
X.520: description	o
X.520: destinationIndicator	o
X.520: facsimileTelephoneNumber	o
X.520: internationalISDNNumber	o
X.520: localityName	o
X.520: organizationalUnitName	m
X.520: physicalDeliveryOfficeName	o
X.520: postalAddress	o
X.520: postalCode	o
X.520: postOfficeBox	o
X.520: preferredDeliveryMethod	o
X.520: registeredAddress	o
X.520: searchGuide	o
X.520: seeAlso	o
X.520: stateOrProvinceName	o
X.520: streetAddress	o
X.520: telephoneNumber	o
X.520: teletexTerminalIdentifier	o
X.520: telexNumber	o
X.509: userPassword	o
X.520: x121Address	o

r. residentialPerson

The residentialPerson object class is not used for Allied Directory entries, but is described in X.521.

4. MHS Standard Structural Object Classes

All of the structural object classes in ITU-T Rec. X.402 | ISO/IEC 10021-2 are used in the Common Content.

a. mhs-distribution-list

The mhs-distribution-list object class is used to define a directory entry that represents a distribution list (DL), that is, an address list that is expanded by the MTS. The attributes in the entry identify the distribution list name, submit permissions, and OR-addresses and, to the extent that the relevant attributes are present, describe the DL, identify its organization, organizational units, and owner; cite related objects; identify its maximum content

length, deliverable content types, and acceptable, exclusively acceptable, and unacceptable encoded information types (EITs); and identify its expansion policy, subscription addresses, archive addresses, related lists and members. Table B-13 shows the composition of the mhs-distribution-list object class. This object class is the base class for MHS Distribution List type directory entries.

Table B-13
mhs-distribution-list Object Class

Attribute	m/o
X.520: commonName	m
X.520: description	o
X.402: mhs-acceptable-eits	o
X.402: mhs-deliverable-content-types	o
X.402: mhs-dl-archive-service	o
X.402: mhs-dl-members	o
X.402: mhs-dl-policy	o
X.402: mhs-dl-related-lists	o
X.402: mhs-dl-submit-permissions	m
X.402: mhs-dl-subscription-service	o
X.402: mhs-exclusively-acceptable-eits	o
X.402: mhs-maximum-content-length	o
X.402: mhs-or-addresses	m
X.402: mhs-unacceptable-eits	o
X.520: organizationalUnitName	o
X.520: organizationName	o
X.520: owner	o
X.520: seeAlso	o

b. mhs-message-store

The mhs-message-store object class is used to define directory entries that represent application entities that implement the MHS MS functionality. The attributes in an entry, to the extent that they are present, describe the MS, identify its owner, and enumerate the attributes, automatic actions, matching rules, content types, and network protocols the MS supports. Table B-14 shows the composition of the mhs-message-store object class. This object class is the base class for MHS Message Store Ed. A type directory entries.

Table B-14
mhs-message-store Object Class

Attribute	m/o
X.520: commonName*	m
X.520: description*	o
X.520: localityName*	o
X.402: mhs-supported-attributes	o
X.402: mhs-supported-automatic-actions	o
X.402: mhs-supported-content-types	o
X.402: mhs-supported-matching-rules	o
X.520: organizationalUnitName*	o
X.520: organizationName*	o
X.520: owner	o
X.520: presentationAddress*	m
X.520: protocolInformation	o
X.520: seeAlso*	o
X.520: supportedApplicationContext*	o

* from applicationEntity (superclass)

c. mhs-message-transfer-agent

The mhs-message-transfer-agent object class is used to define directory entries that represent application entities that implement the MHS MTA functionality. The attributes in an entry, to the extent that they are present, describe the MTA and identify its owner, the maximum content length it can handle, and its supported network protocols. Table B-15 shows the composition of the mhs-message-transfer-agent object class. This object class is the base class for MHS Message Transfer Agent Ed. A type directory entries and is the superclass of the base class for Messaging Gateway Ed. A type directory entries.

Table B-15
mhs-message-transfer-agent Object Class

Attribute	m/o
X.520: commonName*	m
X.520: description*	o
X.520: localityName*	o
X.402: mhs-maximum-content-length	o
X.520: organizationalUnitName*	o
X.520: organizationName*	o
X.520: owner	o
X.520: presentationAddress*	m
X.520: protocolInformation	o
X.520: seeAlso*	o
X.520: supportedApplicationContext*	o

* from applicationEntity (superclass)

d. mhs-user-agent

The mhs-user-agent object class is used to define directory entries that represent application entities that implement the MHS UA functionality. The attributes in an entry, to the extent that they are present, identify the UA's owner; the maximum content length, content types, and EITs it can handle; its deliverable classes; its OR-address; and its supported network protocols. Table B-16 shows the composition of the mhs-user-agent object class. This object class is the base class for MHS User Agent type directory entries.

Table B-16
mhs-user-agent Object Class

Attribute	m/o
X.520: commonName*	m
X.520: description*	o
X.520: localityName*	o
X.402: mhs-acceptable-eits	o
X.402: mhs-deliverable-classes	o
X.402: mhs-deliverable-content-types	o
X.402: mhs-exclusively-acceptable-eits	o
X.402: mhs-maximum-content-length	o
X.402: mhs-or-addresses	o
X.402: mhs-unacceptable-eits	o
X.520: organizationalUnitName*	o
X.520: organizationName*	o
X.520: owner	o
X.520: presentationAddress*	m
X.520: protocolInformation	o
X.520: seeAlso*	o
X.520: supportedApplicationContext*	o

* from applicationEntity (superclass)

5. ACP 133 Structural Object Classes

a. Base Object Classes

The structural object classes of Allied Directory Entries, specified in this annex, for Common Content are:

- aCPNetworkEdB
- aCPNetworkInstructionsEdB
- addressList
- aliasCommonName
- aliasOrganizationalUnit
- altSpellingACP127
- cadACP127

- distributionCodeDescription
- dSSCSPLA
- messagingGateway
- mLA
- mLAgent
- network
- networkInstructions
- orgACP127
- plaCollectiveACP127
- releaseAuthorityPerson
- releaseAuthorityPersonA
- routingIndicator
- sigintPLA
- sIPLA
- spotPLA
- taskForceACP127
- tenantACP127

b. Superclasses

Each of these auxiliary object classes, specified in this ACP (see paragraph 7), is used in the Common Content as a superclass in the definition of a structural object class defined in this ACP:

- plaACP127
- plaData
- secure-user
- securePkiUser

c. aCPNetworkEdB

The aCPNetworkEdB structural object class is used to define directory entries representing interconnected communications networks. This object class replaces the network object class. Table B-17 shows the composition of the aCPNetworkEdB object class. This is the base class for Network EdB type directory entries. A Network EdB entry can have subordinate entries that define the access and instructions for reaching other networks.

Table B-17
aCPNetworkEdB Object Class

Attribute	m/o
X.520: commonName	m
X.520: description	o
ACP 133: aCPNetworkSchemaEdB	o
ACP 133: operationName	o
X.520: seeAlso	o

d. aCPNetworkInstructionsEdB

The aCPNetworkInstructionsEdB structural object class is used to define a directory entry that provides the description of how to reach the subject network from another network. Table B-18 shows the composition of the aCPNetworkInstructionsEdB object class. This object class is the base class for Network Instructions EdB type directory entries.

Table B-18
aCPNetworkInstructionsEdB Object Class

Attribute	m/o
ACP 133: accessCodes	o
ACP 133: aCPNetwAccessSchemaEdB	o
X.520: commonName*	m
X.520: description*	o
ACP 133: networkDN	o

e. addressList

The addressList object class is used to define directory entries that represent address lists, in particular, the members of the list. The sender of a message uses the address list name to

send to all of the members in the list. The replacement of the address list name by the members of the list is performed by the sending UA or an MLA, instead of the MTS. Table B-19 shows the composition of the addressList object class. This object class is the base class for Address List Ed. A type directory entries.

Table B-19
addressList Object Class

Attribute	m/o
X.520: businessCategory	o
X.520: commonName	m
ACP 133: copyMember	o
X.520: description	o
X.520: member	o
X.402: mhs-dl-archive-service	o
X.402: mhs-dl-policy	o
X.402: mhs-dl-related-lists	o
X.402: mhs-dl-submit-permissions	m
X.402: mhs-dl-subscription-service	o
ACP 133: aLExemptedAddressProcessor	o
ACP 133: alid	o
ACP 133: aLReceiptPolicy	o
ACP 133: aLType	o
X.520: organizationalUnitName	o
X.520: organizationName	o
X.520: owner	o
ACP 133: remarks	o
X.520: seeAlso	o

f. aliasCommonName

The aliasCommonName object class is used for an alias entry named by commonName. This permits, for example, an additional name to be given to a person, role, or address list. Table B-20 shows the composition of the aliasCommonName object class. This object class is the base class for Address List Alias, Organizational Person Alias, and Organizational Role Alias type directory entries.

Table B-20
aliasCommonName Object Class

Attribute	m/o
X.501: aliasedEntryName*	m
X.520: commonName	m

* from alias (superclass)

g. aliasOrganizationalUnit

The aliasOrganizationalUnit object class is used for an alias entry named by organizationalUnit. This permits an additional name to be given to a suborganization. Table B-21 shows the composition of the aliasOrganizationalUnit object class. This object class is the base class for Messaging Organizational Unit Alias and Organizational Unit Alias type directory entries.

Table B-21
aliasOrganizationalUnit Object Class

Attribute	m/o
X.501: aliasedEntryName*	m
X.520: organizationalUnitName	m

* from alias (superclass)

h. altSpellingACP127

The altSpellingACP127 object class is used to represent an alternative spelling for a PLA and always contains a reference to the PLA for which it provides an alternate spelling. This object class is a subclass of the plaACP127 auxiliary object class, defined in this ACP. Table B-22 shows the composition of the altSpellingACP127 object class. This object class is the base class for Alternate Spelling PLA type directory entries.

Table B-22
altSpellingACP127 Object Class

Attribute	m/o
ACP 133: community*	o
ACP 133: effectiveDate*	o
ACP 133: expirationDate*	o
ACP 133: nationality*	o
ACP 133: plaNameACP127*	m
ACP 133: plaReplace	m
ACP 133: primarySpellingACP127	m
ACP 133: publish*	o
ACP 133: remarks*	o
ACP 133: serviceOrAgency*	o

* from plaACP127 (superclass); see paragraph 7 in this annex

i. cadACP127

The cadACP127 (Collective Address Designator) object class is used to represent an ACP 127/JANAP 128 distribution list. It is a subclass of the plaACP127 auxiliary object class, defined in this ACP. Table B-23 shows the composition of the cadACP127 object class. This object class is the base class for CAD PLA type directory entries.

Table B-23
cadACP127 Object Class

Attribute	m/o
ACP 133: associatedAL	o
ACP 133: cognizantAuthority	m
ACP 133: community*	o
ACP 133: effectiveDate*	o
ACP 133: entryClassification	o
ACP 133: expirationDate*	o
ACP 133: nationality*	o
ACP 133: plaNameACP127*	m
ACP 133: publish*	o
ACP 133: recapDueDate	o
ACP 133: remarks*	o
ACP 133: rIInfo	o
ACP 133: serviceOrAgency*	o

* from plaACP127 (superclass); see paragraph 7 in this annex

j. distributionCodeDescription

The distributionCodeDescription object class is used to define a directory entry that represents a registered Distribution Code in the directory and describes its meaning. See ACP 123 for specification of distribution codes. The distribution code is held in the commonName attribute. Table B-24 shows the composition of the distributionCodeDescription object class. This object class is the base class for Distribution Code Description type directory entries.

Table B-24
distributionCodeDescription Object Class

Attribute	m/o
X.520: commonName	m
X.520: description	o

k. dSSCSPLA

The dSSCSPLA object class is used to represent an Intelligence Community (IC) Plain Language Address (PLA) organization that, in the directory, is named using the plaNameACP127 attribute. B-25 shows the composition of the dSSCSPLA object class. This object class is the base class for DSSCS PLA type directory entries.

Table B-25
dSSCSPLA Object Class

Attribute	m/o
ACP 133: adminConversion	o
ACP 133: associatedOrganization	o
ACP 133: community*	o
ACP 133: effectiveDate*	o
ACP 133: expirationDate*	o
X.520: localityName	o
ACP 133: nationality*	o
ACP 133: plaNameACP127*	m
ACP 133: publish*	o
ACP 133: remarks*	o
ACP 133: rI	m
ACP 133: serviceOrAgency*	o
ACP 133: sigad	o
ACP 133: usdConversion	o

* from plaACP127 (superclass); see paragraph 7 in this annex

l. messagingGateway

The messagingGateway object class is used to store information about an application entity which serves as an application layer gateway between two mail systems. When a gateway performs translation services, a messagingGateway object provides a mechanism to address these translation services directly. Table B-26 shows the composition of the messagingGateway object class. This object class is the base class for Messaging Gateway Ed. A type directory entries.

Table B-26
messagingGateway Object Class

Attribute	m/o
ACP 133: administrator	o
ACP 133: aigsExpanded	o
X.520: commonName*	m
X.520: description*	o
ACP 133: gatewayType	o
ACP 133: ghpType	o
RFC 1274: host	o
X.520: localityName*	o
ACP 133: mailDomains	o
X.402: mhs-acceptable-eits	o
X.402: mhs-deliverable-content-types	o
X.402: mhs-exclusively-acceptable-eits	o
X.402: mhs-maximum-content-length*	o
X.402: mhs-message-store-dn	o
X.402: mhs-or-addresses	o
X.402: mhs-or-addresses-with-capabilities	o
X.402: mhs-unacceptable-eits	o
ACP 133: onSupported	o
X.520: organizationalUnitName*	o
X.520: organizationName*	o
X.520: owner*	o
ACP 133: plaNameACP127	o
X.520: presentationAddress*	m
X.520: protocolInformation*	o
ACP 133: rIInfo	o
X.520: seeAlso*	o
X.520: supportedApplicationContext*	o

* from mhs-message-transfer-agent (superclass)

m. mLA

(1) The mLA object class is used to represent an application entity that performs the functions of a MLA. This object class is a subclass of applicationEntity and strongAuthenticationUser. Table B-27 shows the composition of the mLA object class.

(2) Note that this object class may be removed from the Common Content in a later edition of this ACP, when the CMI requirements have been more fully established.

Table B-27
mLA Object Class

Attribute	m/o
X.520: commonName*	m
X.520: description*	o
X.520: localityName*	o
X.520: organizationalUnitName*	o
X.520: organizationName*	o
X.520: presentationAddress*	m
X.520: seeAlso*	o
X.509: supportedAlgorithms	o
X.520: supportedApplicationContext*	o
X.509: userCertificate**	m

* from applicationEntity (superclass)

** from strongAuthenticationUser (superclass)

n. mLAgent

The mLAgent object class is used to represent an application entity that performs the functions of a MLA. This object class is a subclass of applicationEntity and pkiUser. Table B-28 shows the composition of the mLAgent object class. This object class is the base class for MLA Ed. A type directory entries.

Table B-28
mLAgent Object Class

Attribute	m/o
X.520: commonName*	m
X.520: description*	o
X.520: localityName*	o
X.520: organizationalUnitName*	o
X.520: organizationName*	o
X.520: presentationAddress*	m
X.520: seeAlso*	o
X.509: supportedAlgorithms	o
X.520: supportedApplicationContext*	o
X.509: userCertificate**	o

* from applicationEntity (superclass)

** from pkiUser (superclass)

o. network

The network structural object class is used to define directory entries representing interconnected communications networks. A Network entry can have subordinate entries that define the access and instructions for reaching other networks. Table B-29 shows the composition of the network object class. This object class is the base class for Network type directory entries. Note that Edition B of this ACP replaces the network object class (which may be removed from this ACP in future editions) with the aCPNetworkEdB object class.

Table B-29
network Object Class

Attribute	m/o
X.520: commonName	m
X.520: description	o
ACP 133: networkSchema	o
ACP 133: operationName	o
X.520: seeAlso	o

p. networkInstructions

The networkInstructions structural object class is used to define a directory entry that provides the description of how to reach the subject network from another network. Table B-30 shows the composition of the networkInstructions object class. This object class is the base class for Network Instructions type directory entries. Note that Edition B of this ACP replaces the networkInstructions object class (which may be removed from this ACP in future editions) with the aCPNetworkInstructionsEdB object class.

Table B-30
networkInstructions Object Class

Attribute	m/o
ACP 133: accessCodes	o
ACP 133: accessSchema	o
X.520: commonName	m
X.520: description	o
ACP 133: networkDN	o

q. orgACP127

The orgACP127 object class is used to define the entry for a single ACP 127/JANAP 128 messaging user. This object class is a subclass of the plaACP127 auxiliary object class, defined in this ACP. Table B-31 shows the composition of the orgACP127 object class. This object class is the base class for Organizational PLA type directory entries.

Table B-31
orgACP127 Object Class

Attribute	m/o
ACP 133: accountingCode	o
ACP 133: associatedOrganization	o
ACP 133: community*	o
X.520: countryName	o
ACP 133: dualRoute	o
ACP 133: effectiveDate*	o
ACP 133: entryClassification	o
ACP 133: expirationDate*	o
X.520: localityName	o
ACP 133: longTitle	o
ACP 133: minimize	o
ACP 133: minimizeOverride	o
ACP 133: nameClassification	o
ACP 133: nationality*	o
ACP 133: plaNameACP127*	m
ACP 133: publish*	o
ACP 133: remarks*	o
ACP 133: rI	o
ACP 133: rIInfo	o
ACP 133: section	o
ACP 133: serviceOrAgency*	o
X.520: stateOrProvinceName	o
ACP 133: tARE	o

* from plaACP127 (superclass); see paragraph 7 in this annex

r. plaCollectiveACP127

The plaCollectiveACP127 object class is used to define the entry for an ACP 127/JANAP 128 Address Indicator Group (AIG) distribution list or Type distribution list. This

object class is a subclass of the plaACP127 auxiliary object class, defined in this ACP. Table B-32 shows the composition of the plaCollectiveACP127 object class. This object class is the base class for PLA Collective type directory entries.

Table B-32
plaCollectiveACP127 Object Class

Attribute	m/o
ACP 133: actionAddressees	o
ACP 133: allowableOriginators	o
ACP 133: associatedAL	o
ACP 133: cognizantAuthority	m
ACP 133: community*	o
X.520: description	o
ACP 133: effectiveDate*	o
ACP 133: entryClassification	o
ACP 133: expirationDate*	o
ACP 133: infoAddressees	o
ACP 133: lastRecapDate	o
ACP 133: nationality*	o
ACP 133: plaNameACP127*	m
ACP 133: publish*	o
ACP 133: recapDueDate	o
ACP 133: remarks*	o
ACP 133: serviceOrAgency*	o

* from plaACP127 (superclass); see paragraph 7 in this annex

s. releaseAuthorityPerson

(1) The releaseAuthorityPerson object class is used to define the entry for a role of release authority who releases organizational messages on behalf of an organization. Whereas organizations originate their organizational messages, it is the job of the release authority to sign the messages. Release authorities do not send individual messages and do not receive messages. Entries for release authorities are subordinate to the entry for the organizationalUnit (that is a messaging user) in the DIT. Table B-33 shows the composition of the releaseAuthorityPerson object class.

(2) Note that this object class may be removed from the Common Content in a later edition of this ACP, when the CMI requirements have been more fully established.

Table B-33
releaseAuthorityPerson Object Class

Attribute	m/o
X.509: attributeCertificate*	o
ACP 133: releaseAuthorityName	m
X.509: supportedAlgorithms*	o
X.509: userCertificate*	m

* from secure-user (superclass); see paragraph 7 in this annex

t. releaseAuthorityPersonA

The releaseAuthorityPersonA object class is used to define the entry for a role of release authority who releases organizational messages on behalf of an organization. Whereas organizations originate their organizational messages, it is the job of the release authority to sign the messages. Release authorities do not send individual messages and do not receive messages. Entries for release authorities are subordinate to the entry for the organizationalUnit (that is a messaging user) in the DIT. Table B-34 shows the composition of the releaseAuthorityPersonA object class. This object class is the base class for Release Authority Person Ed. A type directory entries.

Table B-34
releaseAuthorityPersonA Object Class

Attribute	m/o
X.509: attributeCertificate*	o
ACP 133: releaseAuthorityName	m
X.509: supportedAlgorithms*	o
X.509: userCertificate*	o

* from securePkiUser (superclass); see paragraph 7 in this annex.

u. routingIndicator

The routingIndicator object class is used to define an entry for a RI and is a subclass of the plaData auxiliary object class, defined in this ACP. Table B-35 shows the composition of the routingIndicator object class. This object class is the base class for Routing Indicator Ed. B type directory entries.

Table B-35
routingIndicator Object Class

Attribute	m/o
ACP 133: community*	o
X.520: description*	o
ACP 133: effectiveDate*	o
ACP 133: expirationDate*	o
ACP 133: lmf	o
X.402: mhs-maximum-content-length	o
ACP 133: nationality	o
ACP 133: publish	o
ACP 133: rI	m
ACP 133: rIClassification	o
ACP 133: sHD	o
ACP 133: tCC	o
ACP 133: transferStation	o
ACP 133: tRC	o

* from plaData (superclass); see paragraph 7 in this annex

v. sigintPLA

The sigintPLA object class is used to represent sensitive Signal Intelligence PLAs. This object class is a subclass of the plaData auxiliary object class, defined in this ACP. Table B-36 shows the composition of the sigintPLA object class. This object class is the base class for Signal Intelligence PLA type directory entries.

Table B-36
sigintPLA Object Class

Attribute	m/o
ACP 133: community*	o
X.520: description*	o
ACP 133: effectiveDate*	o
ACP 133: expirationDate*	o
X.520: localityName	o
ACP 133: nationality	o
ACP 133: publish	o
ACP 133: remarks	o
ACP 133: rI	o
ACP 133: shortTitle	o
ACP 133: sigad	m

* from plaData (superclass); see paragraph 7 in this annex

w. sIPLA

The sIPLA object class is used to define the entry for a single Special Intelligence (SI) messaging user. This object class is a subclass of the plaData auxiliary object class, defined in this ACP. Table B-37 shows the composition of the sIPLA object class. This object class is the base class for Special Intelligence PLA type directory entries.

Table B-37
sIPLA Object Class

Attribute	m/o
ACP 133: community*	o
X.520: description*	o
ACP 133: effectiveDate*	o
ACP 133: expirationDate*	o
X.520: localityName	o
ACP 133: longTitle	m
ACP 133: nationality	o
ACP 133: publish	o
ACP 133: remarks	o
ACP 133: rI	o
ACP 133: shortTitle	o
ACP 133: sigad	o

* from plaData (superclass); see paragraph 7 in this annex

x. spotPLA

The spotPLA object class is used to define an entry for a special products distribution list. This object class is a subclass of the plaData auxiliary object class, defined in this ACP. Table B-38 shows the composition of the spotPLA object class. This object class is the base class for SPOT PLA type directory entries.

Table B-38
spotPLA Object Class

Attribute	m/o
ACP 133: actionAddressees	o
ACP 133: additionalAddressees	o
ACP 133: additionalSecondPartyAddressees	o
ACP 133: community*	o
X.520: description*	o
ACP 133: effectiveDate*	o
ACP 133: expirationDate*	o
X.402: mhs-dl-submit-permissions	o
ACP 133: remarks	o
ACP 133: secondPartyAddressees	o
ACP 133: spot	m

* from plaData (superclass); see paragraph 7 in this annex

y. taskForceACP127

The taskForceACP127 object class is used to define a directory entry for an ACP 127/JANAP 128 task force distribution list. This object class is a subclass of the plaACP127 auxiliary object class, defined in this ACP. Table B-39 shows the composition of the taskForceACP127 object class. This object class is the base class for Task Force PLA type directory entries.

Table B-39
taskForceACP127 Object Class

Attribute	m/o
ACP 133: associatedAL	o
ACP 133: cognizantAuthority	m
ACP 133: community*	o
ACP 133: effectiveDate*	o
ACP 133: entryClassification	o
ACP 133: expirationDate*	o
ACP 133: lastRecapDate	m
ACP 133: nationality*	o
ACP 133: plaAddressees	o
ACP 133: plaNameACP127*	m
ACP 133: publish*	o
ACP 133: recapDueDate	m
ACP 133: remarks*	o
ACP 133: serviceOrAgency*	o

* from plaACP127 (superclass); see paragraph 7 in this annex

z. tenantACP127

The tenantACP127 object class is used to define a directory entry that represents a tenant PLA. This object class is a subclass of the plaACP127 auxiliary object class, defined in this ACP, and contains the reference to the host PLA for this tenant. Table B-40 shows the composition of the tenantACP127 object class. This object class is the base class for Tenant PLA type directory entries.

Table B-40
tenantACP127 Object Class

Attribute	m/o
ACP 133: community*	o
ACP 133: effectiveDate*	o
ACP 133: entryClassification	o
ACP 133: expirationDate*	o
ACP 133: hostOrgACP127	m
ACP 133: nationality*	o
ACP 133: plaNameACP127*	m
ACP 133: publish*	o
ACP 133: remarks*	o
ACP 133: serviceOrAgency*	o
ACP 133: tARE	o

* from plaACP127 (superclass); see paragraph 7 in this annex

6. Name Forms and DIT Structural Rules

a. The RDN of each Allied Directory entry is the distinguished value of the naming attribute(s) specified by the Name Form for the structural object class on which the directory entry is based. Although all of the directory standard name forms shall be supported for the Allied Directory System, the standard name forms used in ACP 133 entries are shown in Table B-41. As summarized in Table B-41, the Allied Directory System employs directory standard name forms as well as name forms specified in this annex.

b. Each nation will construct its own structure rules.

Table B-41
Name Forms

Structural Object Class	Naming Attribute	Name Form
aCPNetworkEdB	commonName	aCPNetworkEdBNameForm
aCPNetworkInstructionsEdB	commonName	aCPNetworkInstrEdBNameForm
addressList	commonName	addressListNameForm
aliasCommonName	commonName	aliasCNNameForm
aliasOrganizationalUnit	organizationalUnitName	aliasOUNameForm
altSpellingACP127	plaNameACP127	alternateSpellingPLANameForm
applicationEntity	commonName and, optionally, dnQualifier	aENameForm
applicationProcess	commonName	applProcessNameForm (X.521)
cadACP127	plaNameACP127	cadPLANameForm

Structural Object Class	Naming Attribute	Name Form
country	countryName	countryNameForm (X.521)
cRLDistributionPoint	commonName	cRLDistPtNameForm (X.521)
device	commonName	deviceNameForm (X.521)
distributionCodeDescription	commonName	distributionCodeDescriptionNameForm
dSA	commonName	dSANameForm (X.521)
dSSCSPLA	plaNameACP127	dSSCSPLANameForm
groupOfNames	commonName	gONNameForm (X.521)
locality	localityName or stateOrProvinceName	locNameForm (X.521) or sOPNameForm (X.521)
messagingGateway	commonName	messagingGatewayNameForm
mhs-distribution-list	commonName	mhs-dLNameForm
mhs-message-store	commonName	mSNameForm
mhs-message-transfer-agent	commonName	mTANameForm
mhs-user-agent	commonName	mUANameForm
mLA	commonName	mLANameForm
mLAgent	commonName	mLAgentNameForm
network	commonName	networkNameForm
networkInstructions	commonName	networkInstructionsNameForm
organization	organizationName and, optionally, dnQualifier	organizationNameForm
organizationalPerson	commonName and, optionally, dnQualifier or organizationalUnitName	qualifiedOrgPersonNameForm
orgACP127	plaNameACP127	organizationalPLANameForm
organizationalRole	commonName and, optionally, dnQualifier	orgRNameForm
organizationalUnit	organizationalUnitName and, optionally, dnQualifier	orgUNameForm
plaCollectiveACP127	plaNameACP127	plaCollectiveNameForm
releaseAuthorityPerson	releaseAuthorityName	releaseAuthorityPersonNameForm
releaseAuthorityPersonA	releaseAuthorityName	releaseAuthorityPersonANameForm
routingIndicator	rI	routingIndicatorNameForm
sigintPLA	sigad	sigintPLANameForm
sIPLA	longTitle	sIPLANameForm
spotPLA	spot	spotPLANameForm
taskForceACP127	plaNameACP127	taskForcePLANameForm
tenantACP127	plaNameACP127	tenantPLANameForm

SECTION III

COMMON AUXILIARY OBJECT CLASSES AND ATTRIBUTES

7. Common Auxiliary Object Classes

The Allied Directory System Common Content includes auxiliary object classes defined in the directory and MHS standards and in this ACP. The Common Content uses the certificationAuthority-V2 and pkiCA auxiliary object classes, specified in X.521 and X.509 and DAM 1 for the 1997 versions, as auxiliary object classes of Allied Directory Entries. The auxiliary object of mhs-user defined in X.402 is also used in the Common Content.

a. Superclasses

Each of these standard classes is used in the Common Content as a superclass in the definition of a standard auxiliary object class, as described below, or of an auxiliary object class defined in this ACP:

- certificationAuthority (Note that this object class may be removed from the Common Content in a later edition of this ACP, when the CMI requirements have been more fully established.)
- pkiUser
- strongAuthenticationUser (Note that this object class may be removed from the Common Content in a later edition of this ACP, when the CMI requirements have been more fully established.)

b. Other Standard Auxiliary Object Classes

The standard auxiliary object classes that are included in the Common Content, but are not used in meeting Allied Directory requirements are:

- deltaCRL
- userSecurityInformation

c. ACP 133-specific Auxiliary Object Classes

The auxiliary object classes for Common Content, specified in this annex, are:

- distributionCodesHandled
- otherContactInformation
- plaACP127
- plaData

- plaUser
- secure-user
- securePkiUser
- ukms

d. certificationAuthority-V2

(1) The certificationAuthority-V2 object class is used in defining directory entries for objects which act as CAs, as defined in ITU-T Rec. X.521 | ISO/IEC 9594-7. Table B-42 shows the composition of the certificationAuthority-V2 object class.

(2) Note that this object class may be removed from the Common Content in a later edition of this ACP, when the CMI requirements have been more fully established.

Table B-42
certificationAuthority-V2 Object Class

Attribute	m/o
X.509: authorityRevocationList*	m
X.509: cACertificate*	m
X.509: certificateRevocationList*	m
X.509: crossCertificatePair*	o
X.509: deltaRevocationList	o

* from certificationAuthority (superclass)

e. deltaCRL

The deltaCRL object class is not used for Allied Directory entries, but is described in X.521 (1997) DAM 1.

f. distributionCodesHandled

The distributionCodesHandled object class provides for identifying the distribution codes (e.g., Subject Indicator Codes (SIC) as defined in NATO Subject Indicator System - publication 3 (NASIS APP-3) and supplements) which are handled, either for action or information, by the object (e.g., organizational role, organizational person, or organizational unit) represented by the directory entry in which this auxiliary is included. Table B-43 shows the composition of the distributionCodesHandled object class.

Table B-43
distributionCodesHandled Object Class

Attribute	m/o
ACP 133: distributionCodeAction	o
ACP 133: distributionCodeInfo	o

g. mhs-user

(1) The mhs-user object class is used in defining directory entries representing MHS users. The attributes in an entry identify the MHS user's OR-address and, to the extent that the relevant attributes are present, identify the maximum content length, content types, and EITs that can be handled by the user; its MS; and its preferred delivery methods. Table B-44 shows the composition of the mhs-user object class.

Table B-44
mhs-user Object Class

Attribute	m/o
X.402: mhs-acceptable-eits	o
X.402: mhs-deliverable-content-types	o
X.402: mhs-exclusively-acceptable-eits	o
X.402: mhs-maximum-content-length	o
X.402: mhs-message-store-dn	o
X.402: mhs-or-addresses	m
X.402: mhs-or-addresses-with-capabilities	o
X.402: mhs-unacceptable-eits	o

(2) If the MHS user has multiple OR-addresses, which have differing deliverability capabilities, then the attributes mhs-deliverable-content-types, mhs-deliverable-eits, and mhs-undeliverable-eits should represent the union of these deliverability capabilities; the attribute mhs-maximum-content-length should contain the largest of the values of this attribute. The capability available at each OR-address can then be determined, when required, from the attribute mhs-or-addresses-with-capabilities.

h. otherContactInformation

The otherContactInformation object class provides for additional telephone, location, and mailbox information in directory entries. Table B-45 shows the composition of the otherContactInformation object class.

Table B-45
otherContactInformation Object Class

Attribute	m/o
ACP 133: aCPMobileTelephoneNumber	o
ACP 133: aCPPagerTelephoneNumber	o
ACP 133: aCPPreferredDelivery	o
ACP 133: mailDomains	o
ACP 133: militaryFacsimileNumber	o
ACP 133: militaryTelephoneNumber	o
ACP 133: proprietaryMailboxes	o
RFC 1274: roomNumber	o
ACP 133: secureFacsimileNumber	o
ACP 133: secureTelephoneNumber	o

i. pkiCA

The pkiCA object class, defined in ITU-T Rec. X.509 | ISO/IEC 9594-8 DAM 1, is used in defining directory entries for Certification Authorities. Table B-46 shows the composition of the pkiCA object class.

Table B-46
pkiCA Object Class

Attribute	m/o
X.509: authorityRevocationList	o
X.509: cACertificate	o
X.509: certificateRevocationList	o
X.509: crossCertificatePair	o

j. pkiUser

The pkiUser object class is used in defining directory entries for objects that include user certificates, as defined in ITU-T Rec. X.509 | ISO/IEC 9594-8 DAM 1. Table B-47 shows the composition of the pkiUser object class.

Table B-47
pkiUser Object Class

Attribute	m/o
X.509: userCertificate	o

k. plaACP127

The plaACP127 object class provides for the general PLA attributes common to general service (GENSER) PLA entries, all of which inherit this class. Table B-48 shows the composition of the plaACP127 object class. This object class is the superclass of the base class for Alternate Spelling PLA, CAD PLA, DSSCS PLA, Organizational PLA, PLA Collective, Task Force PLA, and Tenant PLA type directory entries.

Table B-48
plaACP127 Object Class

Attribute	m/o
ACP 133: community	o
ACP 133: effectiveDate	o
ACP 133: expirationDate	o
ACP 133: nationality	o
ACP 133: plaNameACP127	m
ACP 133: publish	o
ACP 133: remarks	o
ACP 133: serviceOrAgency	o

l. plaData

The plaData object class contains attributes common to SI PLAs. Table B-49 shows the composition of the plaData object class. This object class is the superclass of the base class for Routing Indicator, Signal Intelligence PLA, Special Intelligence PLA, and SPOT PLA type directory entries.

Table B-49
plaData Object Class

Attribute	m/o
ACP 133: community	o
X.520: description	o
ACP 133: effectiveDate	o
ACP 133: expirationDate	o

m. plaUser

The plaUser object class contains the name of a PLA's directory entry and, optionally, RI for addressing that PLA. Table B-50 shows the composition of the plaUser object class.

Table B-50
plaUser Object Class

Attribute	m/o
ACP 133: plaNameACP127	m
ACP 133: rIInfo	o

n. secure-user

(1) The secure-user object class is used in defining directory entries that include credentials for ACP 123 users. It is a subclass of the strongAuthenticationUser object class, defined in X.521, which provides for a user certificate. Table B-51 shows the composition of the secure-user object class.

(2) Note that this object class may be removed from the Common Content in a later edition of this ACP, when the CMI requirements have been more fully established.

Table B-51
secure-user Object Class

Attribute	m/o
X.509: attributeCertificate	o
X.509: supportedAlgorithms	o
X.509: userCertificate*	m

* from strongAuthenticationUser (superclass)

o. securePkiUser

The securePkiUser object class is used in defining directory entries that include credentials for ACP 123 users. It is a subclass of the pkiUser object class, defined in X.509 DAM 1, which provides for a user certificate. Table B-52 shows the composition of the securePkiUser object class.

Table B-52
securePkiUser Object Class

Attribute	m/o
X.509: attributeCertificate	o
X.509: supportedAlgorithms	o
X.509: userCertificate*	o

* from pkiUser (superclass)

p. ukms

The ukms object class contains the monthly values of user keying material (UKM) used in the construction of selected CCEB symmetric confidentiality algorithms. Table B-53 shows the composition of the ukms object class.

Table B-53
ukms Object Class

Attribute	m/o
ACP 133: janUKMs	o
ACP 133: febUKMs	o
ACP 133: marUKMs	o
ACP 133: aprUKMs	o
ACP 133: mayUKMs	o
ACP 133: junUKMs	o
ACP 133: julUKMs	o
ACP 133: augUKMs	o
ACP 133: sepUKMs	o
ACP 133: octUKMs	o
ACP 133: novUKMs	o
ACP 133: decUKMs	o

q. userSecurityInformation

The userSecurityInformation object class is not used for Allied Directory entries, but is described in X.521 (1997).

8. Attributes in Common Content Object Classes

This paragraph lists the attributes that are included in the structural and auxiliary object classes in the Common Content. Paragraph 9 gives the attributes in the Common Content that can be added by content rules. The attributes are defined in the Directory and MHS standards, in RFC 1274, and in this ACP. All of the attributes used in the Common Content are described in Section IX of this annex.

a. Directory Standard Attributes

The attributes in the Common Content that are defined in the directory standards and are used to meet Allied Directory requirements are:

- aliasedEntryName
- attributeCertificate
- authorityRevocationList
- businessCategory
- caCertificate
- certificateRevocationList
- commonName
- countryName
- postalAddress
- postalCode
- postOfficeBox
- preferredDeliveryMethod
- presentationAddress
- protocolInformation
- registeredAddress
- roleOccupant

- crossCertificatePair
- deltaRevocationList
- description
- destinationIndicator
- distinguishedName
- facsimileTelephoneNumber
- internationalISDNNumber
- knowledgeInformation
- localityName
- member
- name
- organizationalUnitName
- organizationName
- owner
- physicalDeliveryOfficeName
- searchGuide
- seeAlso
- serialNumber
- stateOrProvinceName
- streetAddress
- supportedAlgorithms
- supportedApplicationContext
- surname
- telephoneNumber
- teletexTerminalIdentifier
- telexNumber
- title
- userCertificate
- userPassword
- x121Address

b. MHS Standard Attributes

The attributes in the Common Content that are defined in the MHS standards are:

- mhs-acceptable-eits
- mhs-deliverable-classes
- mhs-deliverable-content-types
- mhs-dl-archive-service
- mhs-dl-members
- mhs-dl-policy
- mhs-dl-related-lists
- mhs-dl-submit-permissions
- mhs-dl-subscription-service
- mhs-exclusively-acceptable-eits
- mhs-maximum-content-length
- mhs-message-store-dn
- mhs-or-addresses
- mhs-or-addresses-with-capabilities
- mhs-supported-attributes
- mhs-supported-automatic-actions
- mhs-supported-content-types
- mhs-supported-matching-rules
- mhs-unacceptable-eits

c. RFC 1274-defined Attributes

The attributes in the Common Content that are defined in RFC 1274 are:

- buildingName
- host
- rfc822Mailbox
- roomNumber

d. ACP 133-defined Attributes

The attributes in the Common Content that are defined in this ACP are:

- accessCodes
- accessSchema
- aCPMobileTelephoneNumber
- aCPNetwAccessSchemaEdB
- aCPNetworkSchemaEdB
- aCPPagerTelephoneNumber
- aCPPreferredDelivery
- accountingCode
- aCPTelephoneFaxNumber
- actionAddressees
- additionalAddressees
- additionalSecondPartyAddressees
- adminConversion
- administrator
- aigsExpanded
- aLExemptedAddressProcessor
- aliasPointer
- alid
- allowableOriginators
- aLReceiptPolicy
- alternateRecipient
- aLType
- aprUKMs
- associatedAL
- associatedOrganization
- associatedPLA
- augUKMs
- cognizantAuthority
- community
- copyMember
- decUKMs
- deployed
- distributionCodeAction
- distributionCodeInfo
- dualRoute
- effectiveDate
- entryClassification
- expirationDate
- febUKMs
- garrison
- listPointer
- lmf
- longTitle
- mailDomains
- marUKMs
- mayUKMs
- militaryFacsimileNumber
- militaryTelephoneNumber
- minimize
- minimizeOverride
- nameClassification
- nationality
- networkDN
- networkSchema
- novUKMs
- octUKMs
- onSupported
- operationName
- plaAddressees
- plaNameACP127
- plaReplace
- plasServed
- positionNumber
- primarySpellingACP127
- proprietaryMailboxes
- publish
- rank
- recapDueDate
- releaseAuthorityName
- remarks
- rI
- rIClassification
- rIInfo
- secondPartyAddressees
- section
- secureFacsimileNumber
- secureTelephoneNumber
- sepUKMs
- serviceNumber
- serviceOrAgency

- gatewayType
- ghpType
- guard
- hostOrgACP127
- infoAddressees
- janUKMs
- julUKMs
- junUKMs
- lastRecapDate
- sHD
- shortTitle
- sigad
- spot
- tARE
- tCC
- transferStation
- tRC
- usdConversion

e. Other Standard Attributes

There are several other standard attributes that are included in the Common Content, but are not used to meet Allied Directory requirements. The other standard attributes are:

- enhancedSearchGuide
- generationQualifier
- givenName
- houseIdentifier
- initials
- uniqueIdentifier
- uniqueMember

9. Attributes Added by Content Rules

The Common Content uses the dnQualifier and the businessCategory attributes from X.520 as additional attributes. The buildingName and rfc822Mailbox attributes from RFC 1274 are additional attributes in the Common Content. The additional attributes for Common Content, specified in this annex, are:

- aCPLegacyFormat
- aliasPointer
- alternateRecipient
- associatedAL
- associatedOrganization

- associatedPLA
- effectiveDate
- expirationDate
- guard
- listPointer
- nationality
- plasServed
- positionNumber
- rank
- remarks
- serviceNumber
- tCCG

10. Collective Attributes

a. These standard attributes from X.520 may be included in a collectiveAttributeSubentry:

- collectiveFacsimileTelephoneNumber
- collectiveInternationalISDNNumber
- collectiveLocalityName
- collectiveOrganizationalUnitName
- collectiveOrganizationName
- collectivePhysicalDeliveryOfficeName
- collectivePostalAddress
- collectivePostalCode
- collectivePostOfficeBox
- collectiveStateOrProvinceName

- collectiveStreetAddress
- collectiveTelephoneNumber
- collectiveTeletexTerminalIdentifier
- collectiveTelexNumber

b. These attributes, defined in this annex, may be included in a collectiveAttributeSubentry:

- collective-mhs-or-addresses
- collectiveMilitaryFacsimileNumber
- collectiveMilitaryTelephoneNumber
- collectiveNationality
- collectiveSecureFacsimileNumber
- collectiveSecureTelephoneNumber

c. Since collective attributes are defined as subtypes of user attributes, they are returned whenever a query is made for the supertype. Thus, the use of collective attributes allows a single point of administration for certain attributes where many entries have the same value. DSAs shall support collective attributes; whether the facility is used is a national matter. Collective attributes that apply to entries which are shadowed shall be passed with the shadowed information.

SECTION IV

APPLYING CONTENT RULES IN THE COMMON CONTENT

11. Common Content

a. The Allied Directory System Common Content is a set of structural and auxiliary object classes and additional attributes that are combined to form a variety of types of directory entries. Content rules defined for any DIT subtree schema dictate the allowed combinations. Suggested combinations are shown in Table B-54. The combinations marked with "•"represent the ACP 133 Edition B example content rules. The combinations marked with "o" represent combinations in the original ACP 133 that are not included in the Edition B content rules. The types of directory entries that are in the Allied Directory System are defined in paragraph 12 of this section.

b. All of the structural object classes, auxiliary object classes, and additional attributes in the Common Content shall be supported.

c. The structural object classes are shown across the top of the table forming the columns of the table. The name of each structural object class is prefixed by the source of its definition. For example, aliasCommonName is defined in ACP 133, and country is defined in X.521.

d. The auxiliary object classes that may be used in a content rule are shown down the left-hand side. The attributes that may also be included in a content rule for a directory entry based on the structural object class are also shown down the left-hand side. Each auxiliary object class and additional attribute is prefixed by the source of its definition.

e. An example of how to read the chart is as follows: the content rule for the structural object class organizationalUnit (the "X.521: organizationalUnit" column) shows that entries based on this class may also belong to the auxiliary object classes: distributionCodesHandled, mhs-user, otherContactInformation, plaUser, securePkiUser, and ukms. Also, the entry may include the aCPLegacyFormat, aliasPointer, alternateRecipient, associatedPLA, deployed, dnQualifier, effectiveDate, expirationDate, garrison, guard, listPointer, nationality, and rfc822Mailbox attributes.

f. In paragraph 205, the suggested content rules are defined using the formal ASN.1 template defined in X.501. National schemas may change or expand these content rules, if necessary, to include nationally specific auxiliary object classes and additional attributes. Attributes may be made mandatory or optional. Also, attributes which are optional in the structural or auxiliary object classes may be precluded in a content rule.

g. Content rules control which attributes may or may not appear in an entry. When, for example, a directory entry for a suborganization is being added to the Allied Directory System DIB, the organizationalUnit structural object class is used. The value of the entry’s objectClass Attribute is set to indicate the entry is of this class. The content rule for organizationalUnit then determines what other auxiliary classes and attributes may be added to increase the attribute types that are allowed or required in the entry. When an auxiliary object class allowed by the content rule is added to the directory entry, the object identifier for the auxiliary object class is also included in the objectClass attribute in the entry. Thus, if the suborganization is also a messaging user, the objectClass attribute in the entry would include at least the two object identifier values: organizationalUnit and mhs-user.

Table B-54
Common Content

Auxiliary Object Classes \ Structural Object Classes	ACP 133: aCPNetworkEdB	ACP 133: aCPNetworkInstructionsEdB	ACP 133: addressList	ACP 133: aliasCommonName	ACP 133: aliasOrganizationalUnit	X.521: applicationEntity	X.521: applicationProcess	X.521: country	X.521: cRLDistributionPoint	X.521: device	ACP 133: distributionCodeDescription	X.521: dSA	X.521: groupOfNames	X.521: locality	ACP 133: messagingGateway	X.402: mhs-distribution-list	X.402: mhs-message-store	X.402: mhs-message-transfer-agent	X.402: mhs-user-agent	ACP 133: mLA	ACP 133: mLAgent	ACP 133: network	ACP 133: networkInstructions	X.521: organization	X.521: organizationalPerson	X.521: organizationalRole	X.521: organizationalUnit	ACP 133: releaseAuthorityPerson	ACP 133: releaseAuthorityPersonA	ACP 133: altSpellingACP127	ACP 133: cadACP127	ACP 133: dSSCSPLA	ACP 133: orgACP127	ACP 133: plaCollectiveACP127	ACP 133: routingIndicator	ACP 133: sigintPLA	ACP 133: sIPLA	ACP 133: sporPLA	ACP 133: taskForceACP127	ACP 133: tenantACP127	X.521: groupOfUniqueNames*	X.521: residentialPerson*
Auxiliary Classes																																									
X.521: certificationAuthority-V2						○																		○			●														
ACP 133: distributionCodesHandled			●																						●		●													
X.402: mhs-user			●																						●		●													
ACP 133: otherContactInformation																									●		●													
X.509: pkiCA						●																			●		●													
ACP 133: plaACP127																																								
ACP 133: plaData																												●												
ACP 133: plaUser															○		○																							
ACP 133: secure-user							○			○		○					●	●						○				○												
ACP 133: securePkiUser							●			●		●			●										●		●													
ACP 133: ukms			●												●										●		●													
Other Standard Auxiliary Object Classes																																								
X.509: deltaCRL																																								
X.521: userSecurityInformation																																								

● denotes a combination as defined in Annex B, paragraph 11
○ denotes a combination as defined in the original ACP 133, but not in later editions
✱ Other Standard Structural Object Class

Table B-54 (cont.)
Common Content

Attributes \ Structural Object Classes	ACP 133: aCPNetworkEdB	ACP 133: aCPNetworkInstructionsEdB	ACP 133: addressList	ACP 133: aliasCommonName	ACP 133: aliasOrganizationalUnit	X.521: applicationEntity	X.521: applicationProcess	X.521: country	X.521: cRLDistributionPoint	X.521: device	ACP 133: distributionCodeDescription	X.521: dSA	X.521: groupOfNames	X.521: locality	ACP 133: messagingGateway	X.402: mhs-distribution-list	X.402: mhs-message-store	X.402: mhs-message-transfer-agent	X.402: mhs-user-agent	ACP 133: mLA	ACP 133: mLAgent	ACP 133: network	ACP 133: networkInstructions	X.521: organization	X.521: organizationalPerson	X.521: organizationalRole	X.521: organizationalUnit	ACP 133: releaseAuthority	ACP 133: releaseAuthorityPersonA	ACP 133: altSpellingACP127	ACP 133: cadACP127	ACP 133: dSSCSPLA	ACP 133: orgACP127	ACP 133: plaCollectiveACP127	ACP 133: routingIndicator	ACP 133: sigintPLA	ACP 133: slPLA	ACP 133: sportPLA	ACP 133: taskForceACP127	ACP 133: tenanACP127	X.521: groupOfUniqueNames*	X.521: residentialPerson*
Additional Attributes																																									
ACP 133: aCPLegacyFormat			●			●			●			●		●											●	●	●	●													
ACP 133: aliasPointer			●			●			●			●		●							○				●	●	●	●													
ACP 133: alternateRecipient			●																						●	●	●	●													
ACP 133: associatedAL																																									
ACP 133: associatedOrganization						●																																			
ACP 133: associatedPLA																												●													
RFC 1274: buildingName																												●													
X.520: businessCategory																										●															
ACP 133: deployed																										●	●	●													
X.520: dnQualifier						●																				●	●	●													
ACP 133: effectiveDate		●	●	●	●	●			●	●	●	●	●	●	●	●	●	●	●	○	●	○	○		●	●	●	●	●	○										
ACP 133: expirationDate		●	●	●	●	●			●	●	●	●	●	●	●	●	●	●	●	○	●	○	○		●	●	●	●	●											
ACP 133: garrison															●																									
ACP 133: guard			●																																					
ACP 133: listPointer			●																																					
ACP 133: nationality																												●													
ACP 133: plasServed															●																									
ACP 133: positionNumber																									●															
ACP 133: rank																									●															
ACP 133: remarks																																								
RFC 1274: rfc822Mailbox			●												●													●													
ACP 133: serviceNumber																									●															
ACP 133: rCGG																																								
Other Standard Attributes																																								
X.520: enhancedSearchGuide																																								
X.520: generationQualifier																																								
X.520: givenName																																								
X.520: houseIdentifier																																								
X.520: initials																																								
X.520: uniqueIdentifier																																								
X.520: uniqueMember																																								

● denotes a combination as defined in Annex B, paragraph 11
○ denotes a combination as defined in the original ACP 133, but not in later editions
✱ Other Standard Structural Object Class

12. Directory Entries

The Allied Directory System contains the following types of directory entries.

a. Address List Ed. A

(1) An Address List Ed. A directory entry provides for a group of users that are named and addressed as a group for messaging purposes. This directory entry should include especially the list address, its security materials, and its members.

(2) This directory entry uses a content rule based on the structural object class, addressList, which is defined in Section XII of this annex. An example of such a content rule is the addressListRuleEdA in this annex. The directory entry may also include the following auxiliary object classes and additional attributes:

- distributionCodesHandled object class, defined in Section XII of this annex
- mhs-user object class, defined in ITU-T Rec. X.402
- plaUser object class, defined in Section XII of this annex
- secure-user object class, defined in Section XII of this annex (Note that this object class may be removed from the Common Content in a later edition of this ACP, when the CMI requirements have been more fully established.)
- securePkiUser, defined in Section XII of this annex
- ukms object class, defined in Section XII of this annex
- aliasPointer attribute, defined in Section XII of this annex
- alternateRecipient attribute, defined in Section XII of this annex
- effectiveDate attribute, defined in Section XII of this annex
- expirationDate attribute, defined in Section XII of this annex
- guard attribute, defined in Section XII of this annex
- listPointer attribute, defined in Section XII of this annex
- rfc822Mailbox attribute, defined in RFC 1274

b. Address List Alias

(1) An Address List Alias directory entry provides for an alternative means of naming and referring to an address list.

(2) This directory entry uses a content rule based on the structural object class, aliasCommonName, which is defined in Section XII of this annex. An example of such a content rule is the aliasCommonNameRule in this annex. The directory entry may also include the additional attributes: effectiveDate and expirationDate, which are defined in this ACP (Section XII of this annex).

(3) The aliasedEntryName attribute value is the name of the Address List Ed. A directory entry.

c. Alternate Spelling PLA

(1) An Alternate Spelling PLA directory entry provides for an alternate spelling of a PLA; it contains a reference to the PLA for which it is an alternate spelling.

(2) This directory entry is based on the structural object class, altSpellingACP127, which is defined in Section XII of this annex.

d. Application Entity Ed. A

(1) An Application Entity Ed. A directory entry provides a means of referring to those aspects of an application process that are pertinent to communications, such as Presentation Service Access Point address. It may also store certificates used for strong authentication. This type of directory entry is used for applications in an Allied communications network.

(2) This directory entry uses a content rule based on the structural object class, applicationEntity, which is defined in ITU-T Rec. X.521. An example of such a content rule is the aCPApplicationEntityRuleEdA in this annex. The directory object may also include the following auxiliary object classes and additional attributes:

- secure-user object class, defined in this ACP, Section XII of this annex (Note that this object class may be removed from the Common Content in a later edition of this ACP, when the CMI requirements have been more fully established.)
- securePkiUser object class, defined in this ACP, Section XII of this annex
- aliasPointer attribute, defined in this ACP, Section XII of this annex
- dnQualifier attribute, defined in ITU-T Rec. X.520
- effectiveDate attribute, defined in this ACP, Section XII of this annex
- expirationDate attribute, defined in this ACP, Section XII of this annex

(3) Note that although the pkiCA auxiliary object class is permitted by the content rule, using it makes the entry a Certification Authority Ed. B entry.

e. Application Process

(1) An Application Process directory entry provides for representing an application process. An application process is an element within a computer system which performs the information processing for a particular application.

(2) This directory entry is based on the structural object class, applicationProcess, which is defined in ITU-T Rec. X.521.

f. CAD PLA

(1) A CAD PLA directory entry provides for naming and referring to an ACP 127/JANAP 128 distribution list. CADs are medium-to-large distribution lists used to address homogeneous activities and which are centrally defined and programmed into AUTODIN switching centers.

(2) This directory entry is based on the structural object class, cadACP127, which is defined in Section XII of this annex.

g. Certification Authority Ed. B

(1) A Certification Authority Ed. B directory entry provides for naming and referring to a CA. It provides the security information of a CA for certificate management.

(2) The naming attributes distinguished values for naming shall comply with paragraph 305.

(3) This directory entry uses any one of the content rules based on the structural object classes: applicationEntity, organization, organizationalUnit, and organizationalRole, which are defined in ITU-T Rec. X.521. Examples of such content rules are the aCPApplicationEntityRuleEdA, aCPOrganizationRuleEdB, aCPOrganizationalUnitRuleEdB, and aCPOrganizationalRoleRuleEdB in this annex. Certification Authority Ed. B directory entries are different from other types of entries in that the pkiCA auxiliary object class, defined in ITU-T Rec. X.521 DAM 1, is included. A Certification Authority Ed. B directory entry may also include the other auxiliary object classes and additional attributes that are permitted by the content rule which governs the entry.

h. Country

(1) A Country directory entry is generally directly under the root of the DIT and provides the first level of the DIT for each and every Ally providing and using the Allied Directory services.

(2) This directory entry is based on the structural object class, country, which is defined in ITU-T Rec. X.521.

i. CRL Distribution Point

(1) A CRL Distribution Point directory entry provides for holding a CRL that is a subset of the complete CRL issued by one CA or that is a combination of CRLs issued by different CAs.

(2) This directory entry uses a content rule based on the structural object class, cRLDistributionPoint, which is defined in ITU-T Rec. X.521. An example of such a content rule is the aCPCRLDistributionPointRule in this annex. The directory entry may also include the additional attributes: aliasPointer, effectiveDate, and expirationDate, which are defined in Section XII of this annex.

j. Device Ed. A

(1) A Device Ed. A directory entry represents a physical unit which can communicate, such as a modem, printer, etc., with optional authentication capability.

(2) This directory entry uses a content rule based on the structural object class, device, which is defined in ITU-T Rec. X.521. An example of such a content rule is the aCPDeviceRuleEdA in this annex. The directory entry may also include the following auxiliary object classes and additional attributes:

- secure-user object class, defined in Section XII of this annex (Note that this object class may be removed from the Common Content in a later edition of this ACP, when the CMI requirements have been more fully established.)
- securePkiUser object class, defined in Section XII of this annex
- aliasPointer attribute, defined in Section XII of this annex
- effectiveDate attribute, defined in Section XII of this annex
- expirationDate attribute, defined in Section XII of this annex

k. Distribution Code Description

(1) A Distribution Code Description directory entry represents a registered Distribution Code in the directory and describes its meaning. The distribution code is the value of the RDN of the directory entry.

(2) This directory entry is based on the structural object class, distributionCodeDescription, which is defined in Section XII of this annex. An example of such a content rule is the distributionCodeDescriptionRule in this annex. The directory entry may also include the additional attributes: aliasPointer, effectiveDate, and expirationDate, which are defined in Section XII of this annex.

l. DSA Ed. A

(1) A DSA Ed. A directory entry provides the addressing and security information for a DSA. It also stores certificates used for strong authentication.

(2) This directory entry uses a content rule based on the structural object class, dSA, which is defined in ITU-T Rec. X.521. An example of such a content rule is the aCPDSARuleEdA in this annex. The directory entry may also include the following auxiliary object classes and additional attributes:

- secure-user object class, defined in Section XII of this annex (Note that this object class may be removed from the Common Content in a later edition of this ACP, when the CMI requirements have been more fully established.)
- securePkiUser object class, defined in Section XII of this annex
- aliasPointer attribute, defined in Section XII of this annex
- effectiveDate attribute, defined in Section XII of this annex
- expirationDate attribute, defined in Section XII of this annex

m. DSSCS PLA

(1) A DSSCS PLA directory entry provides for a single IC legacy messaging organization.

(2) This directory entry is based on the structural object class, dSSCSPLA, which is defined in Section XII of this annex.

n. Group of Names

(1) A Group of Names directory entry defines an unordered set of DNs which represent individual directory entries or other groups of names. The membership of a group is static, i.e., it is explicitly modified by administrative action, rather than dynamically determined each time reference is made to the group. Group of Names directory entries are useful in constructing access control lists.

(2) This directory entry uses a content rule based on the structural object class, groupOfNames, which is defined in ITU-T Rec. X.521. An example of such a content rule is the aCPGroupOfNamesRule in this annex. The directory entry may also include the additional attributes: aliasPointer, effectiveDate, and expirationDate, which are defined in Section XII of this annex.

o. Group of Unique Names

A Group of Unique Names directory entry is based on the structural object class, groupOfUniqueNames, but is not used to meet Allied Directory requirements.

p. Locality

(1) A Locality directory entry provides for accessing entries that are referred to by a locality-named subtree in the DIT.

(2) This directory entry uses a content rule based on the structural object class, locality, which is defined in ITU-T Rec. X.521. An example of such a content rule is the aCPLocalityRule in this annex. The directory entry may also include the additional attributes: aliasPointer, effectiveDate, and expirationDate, which are defined in Section XII of this annex.

q. Messaging Gateway Ed. A

(1) A Messaging Gateway Ed. A directory entry stores information about an Allied MMHS messaging gateway component that translates message content types, which may include RFC 822, ACP 127/JANAP 128, P22, P2, P772, and ACP 120. It also stores certificates used for strong authentication.

(2) This directory entry uses a content rule based on the structural object class, messagingGateway, which is defined in Section XII of this annex. An example of such a content rule is the messagingGatewayRuleEdA in this annex. The directory entry may also include the following auxiliary object classes and additional attributes:

- secure-user object class, defined in Section XII of this annex (Note that this object class may be removed from the Common Content in a later edition of this ACP, when the CMI requirements have been more fully established.)
- securePkiUser object class, defined in Section XII of this annex
- ukms object class, defined in Section XII of this annex
- aliasPointer attribute, defined in Section XII of this annex
- effectiveDate attribute, defined in Section XII of this annex
- expirationDate attribute, defined in Section XII of this annex
- guard attribute, defined in Section XII of this annex
- plasServed attribute, defined in Section XII of this annex
- rfc822Mailbox attribute, defined in RFC 1274

r. Messaging Organizational Unit Alias

(1) An Messaging Organizational Unit Alias directory entry provides for an alternative means of naming and referring to a suborganization as a messaging user.

(2) This directory entry uses a content rule based on the structural object class, aliasOrganizationalUnit, which is defined in Section XII of this annex. An example of such a content rule is the aliasOrganizationalUnitRule in this annex. The directory entry may also include the additional attributes: effectiveDate and expirationDate, which are defined in Section XII of this annex.

(3) The aliasedEntryName attribute value is the name of the Organizational Unit directory entry that includes the mhs-user auxiliary object class.

s. MHS Distribution List

(1) An MHS Distribution List directory entry represents an AL that is expanded by the MHS. The attributes in this type of entry identify the common name, submit permissions, and OR-addresses of the address list and, to the extent that the relevant attributes are present, describe the address list, identify its organization, organizational units, and owner; cite related objects; identify its maximum content length, deliverable content types, and acceptable, exclusively acceptable, and unacceptable EITs; and identify the expansion policy, subscription addresses, archive addresses, related lists, and members of the AL.

(2) This directory entry uses a content rule based on the structural object class, mhs-distribution-list, which is defined in ITU-T Rec. X.402. An example of such a content rule is the aCPMhs-distribution-listRule in this annex. The directory entry may also include the additional attributes: aliasPointer, effectiveDate, and expirationDate, which are defined in Section XII of this annex.

t. MHS Message Store Ed. A

(1) An MHS Message Store Ed. A directory entry stores information about an Allied MMHS MS component to describe the message store, identify its owner, and enumerate the attributes, automatic actions, matching rules, and content types the MS supports. It also stores certificates used for strong authentication.

(2) This directory entry uses a content rule based on the structural object class, mhs-message-store, which is defined in ITU-T Rec. X.402. An example of such a content rule is the aCPMhs-message-storeRuleEdA in this annex. The directory entry may also include the following auxiliary object classes and additional attributes:

- secure-user object class, defined in Section XII of this annex (Note that the secure-user object class may be removed from the Common Content in a later edition of this ACP, when the CMI requirements have been more fully established.)
- securePkiUser object class, defined in Section XII of this annex
- aliasPointer attribute, defined in Section XII of this annex

- effectiveDate attribute, defined in Section XII of this annex
- expirationDate attribute, defined in Section XII of this annex

u. MHS Message Transfer Agent Ed. A

(1) An MHS Message Transfer Agent Ed. A directory entry stores information about an Allied MMHS MTA component to describe the MTA and identify its owner and its deliverable content length. It may also store certificates used for strong authentication.

(2) This directory entry uses a content rule based on the structural object class, mhs-message--transfer-agent, which is defined in ITU-T Rec. X.402. An example of such a content rule is the aCPMhs-message-transfer-agentRuleEdA in this annex. The directory entry may also include the following auxiliary object classes and additional attributes:

- secure-user object class, defined in Section XII of this annex (Note that this object class may be removed from the Common Content in a later edition of this ACP, when the CMI requirements have been more fully established.)
- securePkiUser object class, defined in Section XII of this annex
- aliasPointer attribute, defined in Section XII of this annex
- effectiveDate attribute, defined in Section XII of this annex
- expirationDate attribute, defined in Section XII of this annex

v. MHS User Agent

(1) An MHS User Agent directory entry stores information about an Allied MMHS UA component to identify the UA's owner; its deliverable content length, content types, and EITs; and its O/R address.

(2) This directory entry uses a content rule based on the structural object class, mhs-user-agent, defined in ITU-T Rec. X.402. An example of such a content rule is the aCPMhs-user-agentRule in this annex. The directory entry may also include the additional attributes: aliasPointer, effectiveDate, and expirationDate, which are defined in Section XII of this annex.

w. MLA Ed. A

(1) An MLA (mail list agent) Ed. A directory entry stores addressing, security, and descriptive information about an Allied MMHS MLA component. It also stores certificates used for strong authentication.

(2) This directory entry uses a content rule based on the structural object class, mLAgent, which is defined in Section XII of this annex. An example of such a content rule is the mLAgentRule in this annex. The directory entry may also include the additional attributes:

aliasPointer, effectiveDate, and expirationDate, which are defined in Section XII of this annex. (Note that the mLAgent object class replaces the mLA object class, which may be removed from the Common Content in a later edition of this ACP, when the CMI requirements have been more fully established.)

x. Network Ed. B

(1) A Network Ed. B directory entry represents a communications network that is connected to other networks that are also represented in the Allied DIB. A Network Ed. B entry can have subordinate entries that define the access to and instructions for reaching other networks.

(2) This directory entry uses a content rule based on the structural object class, aCPNetworkEdB, which is defined in Section XII of this annex. An example of such a content rule is the networkEdBRule in this annex. The directory entry may also include the additional attributes: effectiveDate and expirationDate, which are defined in Section XII of this annex.

y. Network Instructions Ed. B

(1) A Network Instructions Ed. B directory entry provides the description of how to reach the subject network from the network represented by the superior entry. When there is a series of networks between the pair being represented, the instructions shall take into account any extra steps that are required.

(2) This directory entry uses a content rule based on the structural object class, aCPNetworkInstructionsEdB, which is defined in Section XII of this annex. An example of such a content rule is the networkInstructionsEdBRule in this annex. The directory entry may also include the additional attributes: effectiveDate and expirationDate, which are defined in Section XII of this annex.

z. Organization Ed. B

(1) An Organization Ed. B directory entry provides the level of the DIT immediately below the Country directory object, for an Ally or for international/multinational organizations such as NATO and is used for locating the entries used in providing and using the Allied Directory services.

(2) This directory entry uses a content rule based on the structural object class, organization, which is defined in ITU-T Rec. X.521. An example of such a content rule is the aCPOrganizationRuleEdB in this annex. The directory entry may also include the auxiliary object class, otherContactInformation, and the additional attributes: dnQualifier, which is defined in ITU-T Rec. X.520, and aCPLegacyFormat, aliasPointer, effectiveDate, and expirationDate, which are defined in Section XII of this annex.

(3) Note that although the pkiCA auxiliary object class is permitted by the content rule, using it makes the entry a Certification Authority Ed. B entry.

aa. Organizational Person Ed. B

(1) An Organizational Person Ed. B directory entry stores information, representing an individual as a member of an organization and, optionally, representing that individual as a user of applications, such as electronic messaging. It also stores certificates used for strong authentication.

(2) This directory entry uses a content rule based on the structural object class, organizationalPerson, which is defined in ITU-T Rec. X.521. An example of such a content rule is the aCPOrganizationalPersonRuleEdB in this annex. The directory entry may also include the following auxiliary object classes and additional attributes:

- distributionCodesHandled object class, defined in Section XII of this annex
- mhs-user object class, defined in ITU-T Rec. X.402
- otherContactInformation object class, defined in Section XII of this annex
- secure-user object class, defined in Section XII of this annex (Note that this object class may be removed from the Common Content in a later edition of this ACP, when the CMI requirements have been more fully established.)
- securePkiUser object class, defined in Section XII of this annex
- ukms object class, defined in Section XII of this annex
- aCPLegacyFormat attribute, defined in Section XII of this annex
- aliasPointer attribute, defined in Section XII of this annex
- alternateRecipient attribute, defined in Section XII of this annex
- businessCategory attribute, defined in ITU-T Rec. X.520
- deployed attribute, defined in Section XII of this annex
- dnQualifier attribute, defined in ITU-T Rec. X.520
- effectiveDate attribute, defined in Section XII of this annex
- expirationDate attribute, defined in Section XII of this annex
- garrison attribute, defined in Section XII of this annex
- guard attribute, defined in Section XII of this annex
- listPointer attribute, defined in Section XII of this annex

- nationality attribute, defined in Section XII of this annex
- positionNumber attribute, defined in Section XII of this annex
- rank attribute, defined in Section XII of this annex
- rfc822MailBox attribute, defined in RFC 1274
- serviceNumber attribute, defined in Section XII of this annex

bb. Organizational Person Alias

(1) An Organizational Person Alias directory entry provides for an alternative means of naming and referring to an organizational person.

(2) This directory entry uses a content rule based on the structural object class, aliasCommonName, which is defined in Section XII of this annex. An example of such a content rule is the aliasCommonNameRule in this annex. The directory entry may also include the additional attributes: effectiveDate and expirationDate, which are defined in Section XII of this annex.

(3) The aliasedEntryName attribute value is the name of the Organizational Person Ed. B directory entry.

cc. Organizational PLA

(1) An Organizational PLA directory entry provides for a single ACP 127/JANAP 128 messaging organization.

(2) This directory entry is based on the structural object class, orgACP127, which is defined in Section XII of this annex.

dd. Organizational Role Ed. B

(1) An Organizational Role Ed. B directory entry stores information representing a role or function, such as, security officer, which is performed by one or more persons. The information includes whatever is needed for the role to participate as a user in applications, such as electronic messaging. It may also store certificates used for strong authentication.

(2) This directory entry uses a content rule based on the structural object class, organizationalRole, which is defined in ITU-T Rec. X.521. An example of such a content rule is the aCPOrganizationalRoleRuleEdB in this annex. The directory entry may also include the following auxiliary object classes and additional attributes:

- distributionCodesHandled object class, defined in Section XII of this annex
- mhs-user object class, defined in ITU-T Rec. X.402

- otherContactInformation object class, defined in Section XII of this annex
- secure-user object class, defined in Section XII of this annex (Note that this object class may be removed from the Common Content in a later edition of this ACP, when the CMI requirements have been more fully established.)
- securePkiUser object class, defined in Section XII of this annex
- ukms object class, defined in Section XII of this annex
- aCPLegacyFormat attribute, defined in Section XII of this annex
- aliasPointer attribute, defined in Section XII of this annex
- alternateRecipient attribute, defined in Section XII of this annex
- businessCategory attribute, defined in ITU-T Rec. X.520
- deployed attribute, defined in Section XII of this annex
- dnQualifier attribute, defined in ITU-T Rec. X.520
- effectiveDate attribute, defined in Section XII of this annex
- expirationDate attribute, defined in Section XII of this annex
- garrison attribute, defined in Section XII of this annex
- guard attribute, defined in Section XII of this annex
- listPointer attribute, defined in Section XII of this annex
- nationality attribute, defined in Section XII of this annex
- rfc822Mailbox attribute, defined in RFC 1274

(3) Note that although the pkiCA auxiliary object class is permitted by the content rule, using it makes the entry a Certification Authority Ed. B entry, see paragraph 12 g. Also, see paragraph 12 ii, Release Authority Role Ed. B.

ee. Organizational Role Alias

(1) An Organizational Role Alias directory entry provides for an alternative means of naming and referring to an organizational role.

(2) This directory entry uses a content rule based on the structural object class, aliasCommonName, which is defined in Section XII of this annex. An example of such a content rule is the aliasCommonNameRule in this annex. The directory entry may also include

the additional attributes: effectiveDate and expirationDate, which are defined in Section XII of this annex.

(3) The aliasedEntryName attribute value is the name of the Organizational Role Ed. B directory entry.

ff. Organizational Unit Ed. B

(1) An Organizational Unit Ed. B directory entry provides a level of the DIT immediately below the Organization Ed. B directory entry of an Ally or another Organizational Unit Ed. B directory entry. An Organizational Unit Ed. B directory entry represents a suborganization and is used for navigating to directory entries belonging to that suborganization, e.g., Organizational Role Ed. B directory entries.

(2) This directory entry uses a content rule based on the structural object class, organizationalUnit, which is defined in ITU-T Rec. X.521. An example of such a content rule is the aCPOrganizationalUnitRuleEdB in this section. The directory entry may also include the following auxiliary object classes and additional attributes:

- distributionCodesHandled object class, defined in Section XII of this annex
- mhs-user object class, defined in ITU-T Rec. X.402
- otherContactInformation object class, defined in Section XII of this annex
- plaUser object class, defined in Section XII of this annex
- secure-user object class, defined in Section XII of this annex (Note that this object class may be removed from the Common Content in a later edition of this ACP, when the CMI requirements have been more fully established.)
- securePkiUser object class, defined in Section XII of this annex
- ukms object class, defined in Section XII of this annex
- aCPLegacyFormat attribute, defined in Section XII of this annex
- aliasPointer attribute, defined in Section XII of this annex
- alternateRecipient attribute, defined in Section XII of this annex
- associatedPLA attribute, defined in Section XII of this annex
- buildingName attribute, defined in RFC 1274
- deployed attribute, defined in Section XII of this annex
- dnQualifier attribute, defined in ITU-T Rec. X.520

- effectiveDate attribute, defined in Section XII of this annex
- expirationDate attribute, defined in Section XII of this annex
- garrison attribute, defined in Section XII of this annex
- guard attribute, defined in Section XII of this annex
- listPointer attribute, defined in Section XII of this annex
- nationality attribute, defined in Section XII of this annex
- rfc822Mailbox attribute, defined in RFC 1274

(3) Note that although the pkiCA auxiliary object class is permitted by the content rule, using it makes the entry a Certification Authority Ed. B entry.

gg. Organizational Unit Alias

(1) An Organizational Unit Alias directory entry provides an alternative means of naming and referring to an organizational unit.

(2) This directory entry uses a content rule based on the structural object class, aliasOrganizationalUnit, which is defined in Section XII of this annex. An example of such a content rule is the aliasOrganizationalUnitRule in this annex. The directory entry may also include the additional attributes: effectiveDate and expirationDate, which are defined in Section XII of this annex.

(3) The aliasedEntryName attribute value is the name of the Organizational Unit Ed. B directory entry.

hh. PLA Collective

(1) A PLA Collective directory entry provides for an ACP 127/JANAP 128 AIG distribution list or Type distribution list. A Type collective is composed of military units of the same type such as destroyers.

(2) This directory entry is based on the structural object class, plaCollectiveACP127, which is defined in Section XII of this annex.

ii. Release Authority Person Ed. A

(1) A Release Authority Person Ed. A directory entry provides the certificate information used by a release authority to sign organizational messages and for strong authentication. The function fulfilled by a Release Authority is defined as a national matter. To validate that the object represented by the directory entry is an authorized Release Authority, the certificate must be checked.

(2) This directory entry type is used by the U.S., where messages are sent to organizations. Because organizational messages are sent to organizations, originators in other countries do not need to query the Allied Directory for a Release Authority. The ability of the originator to release organizational messages is checked by examining the certificate.

(3) This directory entry uses a content rule based on the structural object class, releaseAuthorityPersonA, which is defined in Section XII of this annex. An example of such a content rule is the rAPersonRuleEdA in this annex. The directory entry may also include the additional attributes: effectiveDate, and expirationDate, which are defined in Section XII of this annex. (Note that the releaseAuthorityPersonA object class replaces the releaseAuthorityPerson object class, which may be removed from the Common Content in a later edition of this ACP, when the CMI requirements have been more fully established.)

jj. Release Authority Role Ed. B

(1) A Release Authority Role Ed. B directory entry provides the certificate information used by a release authority to send and receive organizational messages and for strong authentication. The function fulfilled by a Release Authority is defined as a national matter. To validate that the object represented by the directory entry is an authorized Release Authority, the certificate must be checked.

(2) The commonName attribute distinguished value for naming shall be “release authority,” as specified in paragraph 307. It is this naming convention that differentiates a Release Authority Role Ed. B entry from other entries that are based on the organizationalRole object class.

(3) This directory entry uses a content rule based on the structural object class, organizationalRole, which is defined in ITU-T Rec. X.521. An example of such a content rule is the aCPOrganizationalRoleRuleEdB in this annex. The directory entry may also include the following auxiliary object classes and additional attributes:

- distributionCodesHandled object class, defined in Section XII of this annex
- mhs-user object class, defined in ITU-T Rec. X.402
- otherContactInformation object class, defined in Section XII of this annex
- secure-user object class, defined in Section XII of this annex (Note that this object class may be removed from the Common Content in a later edition of this ACP, when the CMI requirements have been more fully established.)
- securePkiUser object class, defined in Section XII of this annex
- ukms object class, defined in Section XII of this annex
- aCPLegacyFormat attribute, defined in Section XII of this annex
- aliasPointer attribute, defined in Section XII of this annex

- alternateRecipient attribute, defined in Section XII of this annex
- deployed attribute, defined in Section XII of this annex
- effectiveDate attribute, defined in Section XII of this annex
- expirationDate attribute, defined in Section XII of this annex
- garrison attribute, defined in Section XII of this annex
- guard attribute, defined in Section XII of this annex
- listPointer attribute, defined in Section XII of this annex
- nationality, defined in Section XII of this annex
- rfc822Mailbox attribute, defined in RFC 1274

kk. Residential Person

A Residential Person directory entry is based on the structural object class, groupOfUniqueNames, but is not used to meet Allied Directory requirements.

ll. Routing Indicator Ed. B

(1) A Routing Indicator Ed. B directory entry provides the description for an ACP 127/JANAP 128 RI.

(2) The directory entry uses a content rule based on the structural object class, routingIndicator, which is defined in Section XII of this annex. An example of such a content rule is the aCPRoutingIndicatorRuleEdB in this annex. The directory entry may also include the additional attributes: remarks, and tCCG, which are defined in Section XII of this annex.

mm. Signal Intelligence PLA

(1) A Signal Intelligence PLA directory entry provides for sensitive SI PLAs.

(2) This directory entry uses a content rule based on the structural object class, sigintPLA, which is defined in Section XII of this annex. An example of such a content rule is the sigintPLARule in this annex. The directory entry may also include the additional attribute: associatedOrganization, which is defined in this ACP (Section XII of this annex).

nn. Special Intelligence PLA

(1) An Special Intelligence PLA directory entry provides for a single SI messaging user of ACP 127/JANAP 128.

(2) The directory entry is based on the structural object class, sIPLA, which is defined in Section XII of this annex.

oo. SPOT PLA

(1) A SPOT PLA directory entry provides for special products distribution lists used in ACP 127/JANAP 128.

(2) This directory entry uses a content rule based on the structural object class, spotPLA, which is defined in Section XII of this annex. An example of such a content rule is the spotPLARule in this annex. The directory entry may also include the additional attribute: associatedAL, which is defined in this ACP (Section XII of this annex).

pp. Task Force PLA

(1) A Task Force PLA directory entry provides the composition and description of an ACP 127/JANAP 128 task force distribution list.

(2) This directory entry is based on the structural object class, taskForceACP127, which is defined in Section XII of this annex.

qq. Tenant PLA

(1) A Tenant PLA directory entry provides the reference to the host PLA for this tenant. An example of a host is a ship and of a tenant, a Marine detachment on the ship.

(2) This directory entry is based on the structural object class, tenantACP127, which is defined in Section XII of this annex.

SECTION V

OBJECT CLASSES HIERARCHY

13. ACP 133-defined Object Classes

The relationship of the object classes, both standard and ACP-defined, included in the Common Content are shown in Figure B-1.

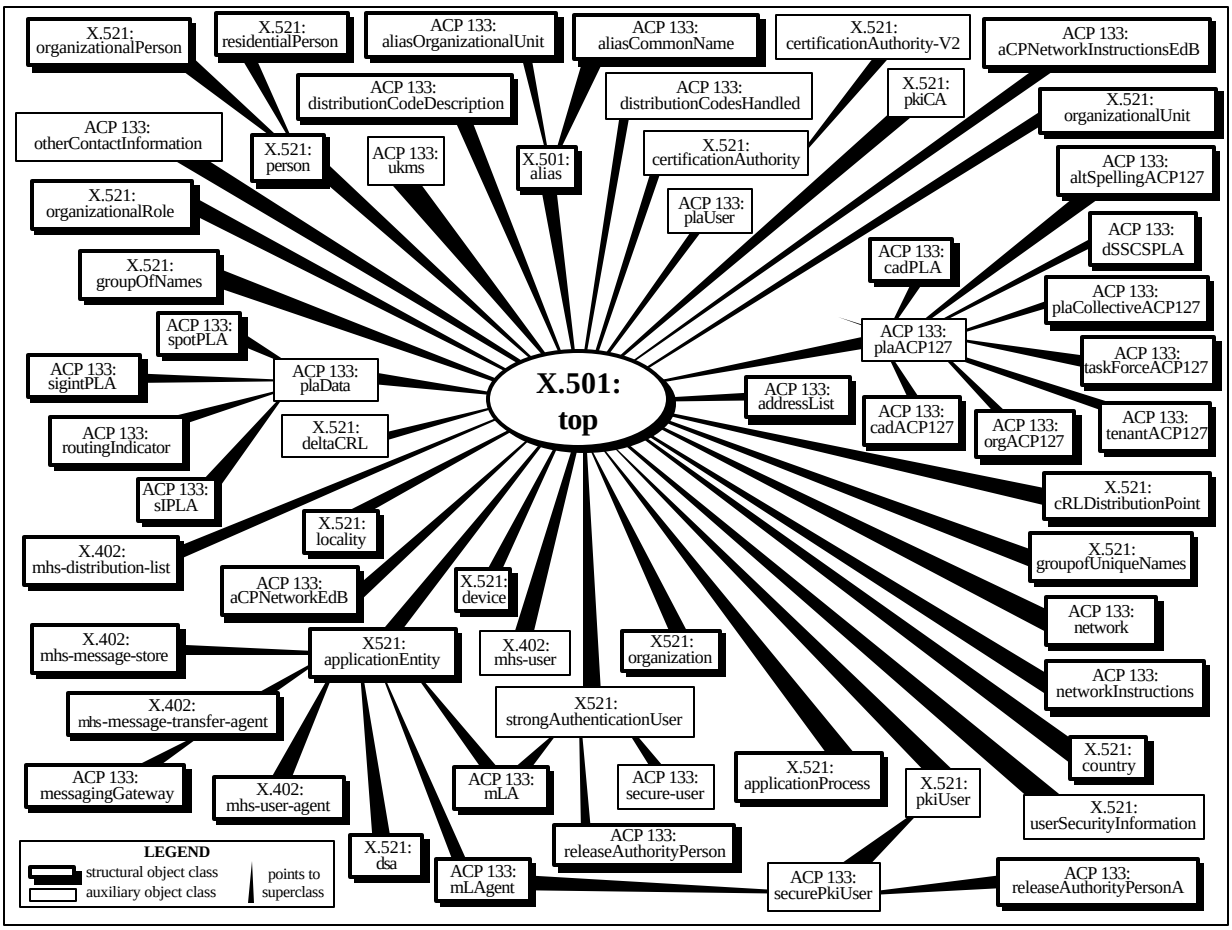

Figure B-1
Hierarchy of Common Content Object Classes

SECTION VI

ATTRIBUTE TYPES HIERARCHY

14. Attribute Subtypes

Figure B-2 shows the attributes in the Common Content that are defined as subtypes of other attributes. This indicates the subtype attributes that may be included in operations involving the parent types.

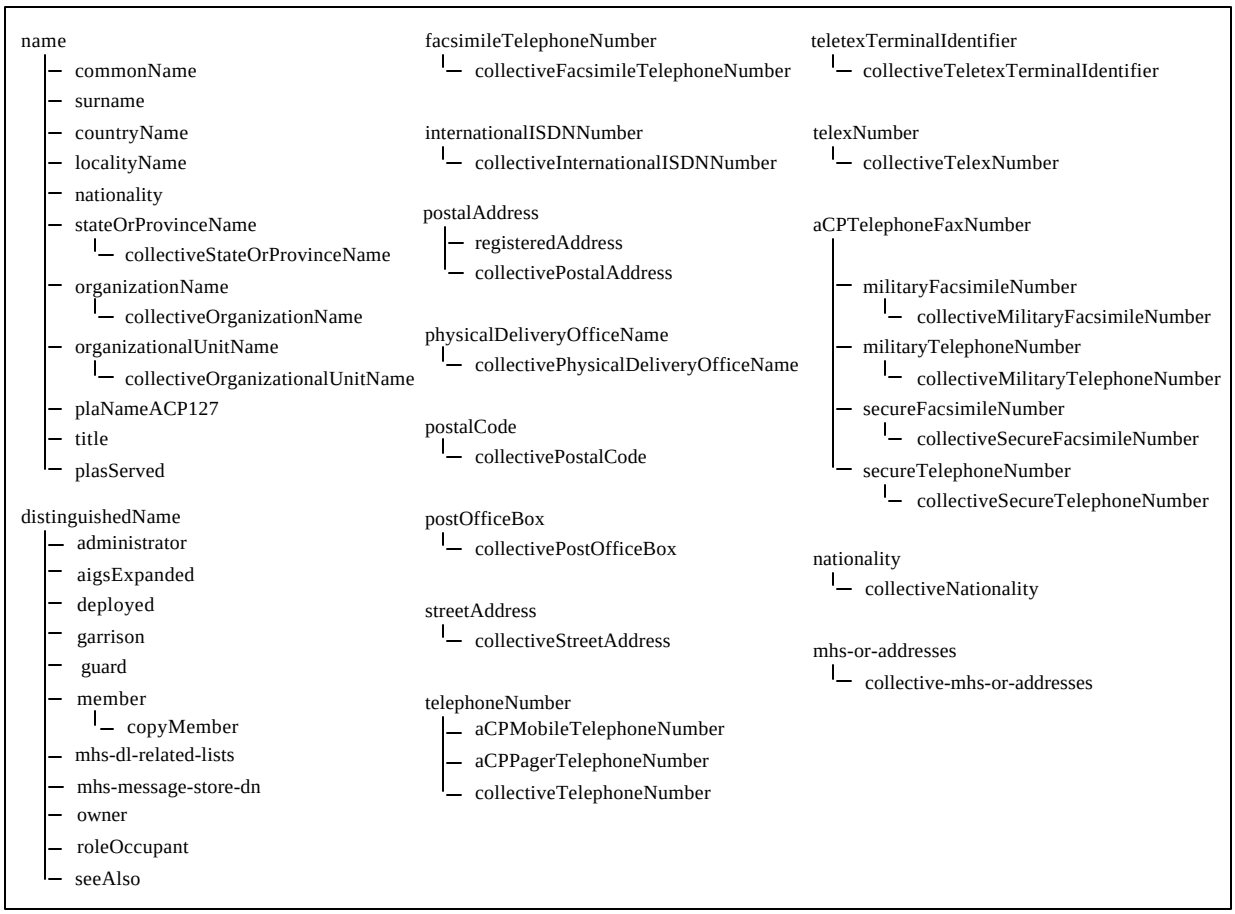

Figure B-2
Attribute Types Defined by Subtyping

SECTION VII

USEFUL OBJECT CLASSES AND NAME FORMS

15. General

There are no object classes defined in this ACP besides the ones included in the Common Content. There are no name forms defined in this ACP besides the ones that apply to the structural object classes included in the Common Content.

SECTION VIII

USEFUL ATTRIBUTES

16. General

a. Some useful attributes have been defined in RFC 1274. Useful attributes defined in paragraph 209 of this Annex are:

- collectiveMilitaryPostalAddress
- collectiveVisitorAddress
- hoursOfOperation
- jpegPhoto
- militaryPostalAddress
- visitorAddress

b. Useful attributes shall not be replicated unless specific bi-lateral arrangements are made for their support on both the supplier and consumer systems.

SECTION IX

ATTRIBUTE DEFINITIONS

17. Common Content

The following paragraphs define the attributes that are included in the Common Content. The definitions of attributes defined in the referenced standards are included for convenience only, and the definitions in those standards take precedence over those given here.

18. accessCodes

a. The accessCodes attribute value gives the coding of how to reach one network from another. Additional instructions for the use of this access code are contained in a description attribute in the same entry. For example, in a private telephone network, the user could be required to dial “8” to reach other users in a different city or to dial “9” to exit the private network.

b. This attribute is defined in this ACP.

19. accessSchema

a. The accessSchema attribute value is a schematic representation used to complete the access information from one network to another in the case of a complex connection. (Many connections are not complex enough to need such a description and in that case the attribute would not be populated.)

b. This attribute is defined in this ACP. Note that this attribute is replaced by the aCPNetwAccessSchemaEdB attribute.

20. accountingCode

a. The accountingCode attribute value is a character string used in logistics applications to identify an organization uniquely. One example is the U.S. Department of Defense Activity Accounting Code (DODAAC).

b. This attribute is defined in this ACP.

21. aCPLegacyFormat

a. The aCPLegacyFormat provides the specific message format type used when the value of the aCPPreferredDelivery attribute is ACP127(1). The values are:

- JANAP 128
- ACP 126
- DOI 103
- DOI 103 Special
- ACP 127
- ACP 127 Converted
- Reserved1 for ACP 127 Standard
- ACP 127 State
- ACP 127 Modified
- SOCOMM Special
- SOCOMM Narrative
- Reserved2 for SOCOMM Narrative TTY
- SOCOMM Narrative Special
- SOCOMM Data
- SOCOMM Internal
- SOCOMM External
- several values for national or bilateral use

b. This attribute is defined in this ACP.

22. aCPMobileTelephoneNumber

a. The aCPMobileTelephoneNumber attribute value identifies a mobile telephone number for the object represented by the directory entry that contains this attribute.

b. This attribute is a subtype of telephoneNumber and is defined in this ACP.

23. aCPNetwAccessSchemaEdB

a. The aCPNetwAccessSchemaEdB attribute value is a schematic representation used to complete the access information from one network to another in the case of a complex connection. (Many connections are not complex enough to need such a description and in that case the attribute would not be populated.)

b. This attribute is defined in this ACP. Note that this attribute replaces the accessSchema attribute.

24. aCPNetworkSchemaEdB

a. The aCPNetworkSchemaEdB attribute value is a graphical representation of a network. It describes the structure of the network and details any rules associated with that network.

b. This attribute is defined in this ACP. Note that this attribute replaces the networkSchema attribute.

25. aCPPagerTelephoneNumber

a. The aCPPagerTelephoneNumber attribute identifies a telephone number for a pager associated with the object represented by the directory entry.

b. This attribute is a subtype of telephoneNumber and is defined in this ACP.

26. aCPPreferredDelivery

a. The aCPPreferredDelivery attribute value is used to determine the messaging system that a user, represented by the directory entry, prefers for message delivery. The possible values are: “ACP127”, “SMTP” or “MHS”. The “MHS” value signifies either standard X.400 (1984 or 1988) or ACP 123-compliant X.400. When the value is "ACP127" more information is given in the aCPLegacyFormat attribute (see paragraph 21 of this annex).

b. This attribute is defined in this ACP.

27. aCPTelephoneFaxNumber

a. The aCPTelephoneFaxNumber attribute is defined for use as a supertype in defining the attributes:

- militaryFacsimileNumber
- militaryTelephoneNumber
- secureFacsimileNumber
- secureTelephoneNumber

b. A value of the aCPTelephoneFaxNumber attribute and the attributes defined as its subtypes is a telephone number that is used for military purposes and is associated with an object represented by the directory entry. For example, a person may have a telephone, equipped with a STU III device, on the Public Switched Telephone Network (PSTN).

c. The attribute value for an ACP telephone number contains the following substrings which are separated by commas (i.e., ","):

- network or site identifier
- telephone number
- security device identifier

(1) The maximum size of the network or site identifier substring is 6 characters. In the example, the string "PSTN" would be the value of this identifier.

(2) For the telephone number substring, if the network is the PSTN, then the format shall be as for a Telephone Number as defined in X.520 (i.e., CCITT E.123). Extension numbers shall be proceeded by "ext." or other nationally defined equivalent. The maximum length of this substring is 32 characters. In the example, the string "+1 555 222 ext. 34" could be the value of the telephone number.

(3) The maximum size of the security device identifier substring is 8 characters. In the example, the string "STU III" would be the value of this identifier.

d. The complete example value would be "PSTN, +1 555 222 ext. 34, STU III".

e. The security device (and preceding substring separator ",") is present only if the military telephone number is secured (i.e., attribute subtypes secureTelephoneNumber or secureFacsimileNumber).

f. Note that the equality and substring matching rule for this attribute is not case sensitive and the substring matching rule is case sensitive. Thus, it is recommended that the network/site identifier and security device identifier are in upper case.

g. This attribute is defined in this ACP.

28. actionAddressees

a. An actionAddressees attribute value is the list of action addressees of an ACP 127/JANAP 128 collective, for example an Address Indicator Group. An action addressee is expected to take appropriate action on the message content, whereas an information addressee receives the message for informational purposes only.

b. This attribute is defined in this ACP.

29. additionalAddressees

a. The additionalAddressees attribute value is a list of addressees to be added to the actionAddressees list (value of the actionAddressees attribute) under circumstances identified in the remarks attribute in the same directory entry.

b. This attribute is defined in this ACP.

30. additionalSecondPartyAddressees

a. The additionalSecondPartyAddressees attribute value is a list of addressees to be added to the secondPartyAddressees list (value of the secondPartyAddressees attribute) under circumstances identified in the remarks attribute in the same directory entry.

b. This attribute is defined in this ACP.

31. adminConversion

a. The adminConversion attribute provides for using an abbreviation of the organization's administrative title as an administrative message address.

b. This attribute is defined in this ACP.

32. administrator

a. The administrator attribute value represents the entity responsible for the operation of a component when it is different from the owner of the component. For example, the owner may be a domain.

b. This attribute is defined in this ACP.

33. aigsExpanded

a. The aigsExpanded attribute values are the names of the AIGs expanded by a messaging gateway.

b. This attribute is defined in this ACP.

34. aLExemptedAddressProcessor

a. The aLExemptedAddressProcessor attribute value is the ORName of the address list's exempted address processor.

b. This attribute is defined in this ACP.

35. aliasedEntryName

a. The aliasedEntryName attribute value contains a name of the directory entry to which the object containing this attribute refers.

b. This attribute is defined in X.501.

36. aliasPointer

a. The aliasPointer attribute type value points to alias directory entries which might have to be modified if the directory entry containing this attribute is modified. It is intended to be used to maintain data consistency in the Directory Information Base (DIB).

b. This attribute is defined in this ACP.

37. alid

a. The alid attribute value is the AL key material identifier.

b. This attribute is defined in this ACP.

38. allowableOriginators

a. The allowableOriginators attribute value is the name of an ACP 127/JANAP 128 collective that contains the list of PLAs that are allowed to originate messages to this list.

b. This attribute is defined in this ACP.

39. aLReceiptPolicy

a. The aLReceiptPolicy attribute value indicates address list's signed receipt policy. This receipt policy supersedes the originator's request for signed receipts (see ACP 120).

b. This attribute is defined in this ACP.

40. alternateRecipient

a. The alternateRecipient attribute is used to designate an X.400 alternate recipient for a messaging user. It could be used by an X.400 message originator to create an originator-assigned alternate recipient address to be used by the message transfer system if delivery to the addressed recipient fails.

b. This attribute is defined in this ACP.

41. aLType

a. The aLType attribute value indicates the type of an address list from these possibilities: AIG (Address Indicator Group), Type Organization Collective, CAD (Collective Address Designator), Task Force, and DAG (DSSCS Address Group).

b. This attribute is defined in this ACP.

42. aprUKMs

a. The aprUKMs (User Key Materials) attribute value is used in the construction of selected CCEB symmetric confidentiality algorithms for the month of April.

b. This attribute is defined in this ACP.

43. associatedAL

a. The associatedAL attribute value points to the address list object which replaces the ACP 127/JANAP 128 Task Force PLA. It assists in the transition from ACP 127/JANAP 128 to X.400 addressing and the associated transition from the use of ACP 127/JANAP 128 collectives to the use of address lists.

b. This attribute is defined in this ACP.

44. associatedOrganization

a. The associatedOrganization attribute value points to the Organizational Unit Ed. B directory entry which represents the same organizational messaging entity as the PLA directory entry containing this attribute.

b. This attribute is defined in this ACP.

45. associatedPLA

a. The associatedPLA attribute value points to the ACP 127/JANAP 128 directory entry for the same messaging entity as represented by the Organizational Unit Ed. B directory entry containing this attribute.

b. This attribute is defined in this ACP.

46. attributeCertificate

a. The attributeCertificate attribute is used to issue new authorizations from a Certification Authority (CA) other than the CA who originally issued the user certificate. The attribute certificate is bound to a user's X.509 certificate but is not part of the originally issued user certificate.

b. This attribute is defined in ITU-T Rec. X.509 (1997).

47. augUKMs

a. The augUKMs attribute value is used in the construction of selected CCEB symmetric confidentiality algorithms for the month of August.

b. This attribute is defined in this ACP.

48. authorityRevocationList

a. The authorityRevocationList value is a time-stamped list of revoked certificates of all CAs known to the CA, certified by the CA.

b. This attribute is defined in X.509.

49. buildingName

a. The buildingName attribute value is the name of the building in which an organizational unit is based.

b. This attribute is defined in RFC 1274.

50. businessCategory

a. The businessCategory attribute value specifies information concerning the occupation of a person, providing the facility for interrogating the directory about people sharing the same occupation.

b. This attribute is defined in X.520.

51. cACertificate

a. The cACertificate attribute of a CA's directory entry shall be used to store self-issued certificates (if any) and certificates issued to this CA by CAs in the same realm as this CA.

b. The definition of realm is purely a matter of local policy.

c. This attribute is defined in X.509.

52. certificateRevocationList

a. The certificateRevocationList attribute value is a time-stamped list of the certificates the Certification Authority issued which have been revoked.

b. This attribute is defined in X.509.

53. cognizantAuthority

a. The cognizantAuthority attribute value indicates the administrator for an ACP 127/JANAP 128 collective.

b. This attribute is defined in this ACP.

54. commonName

a. A commonName attribute value is an identifier of a person, role, or other object. A Common Name is not necessarily part of a directory name although this attribute is used in naming in the Allied Directory DIT. A Common Name is a (possibly ambiguous) name by which the object is commonly known in some limited scope (such as an organization) and conforms to the naming conventions of the country or culture with which it is associated. For example:

- commonName = “Eisenhower, Dwight”
- commonName = “Divisional Commander”
- commonName = “High Speed Modem”

b. Any variants associated with the named object are separate and alternative attribute values (i.e., the commonName attribute is multi-valued in the object’s entry).

c. This attribute is defined in X.520.

55. community

a. The community attribute value indicates whether an object belongs to the GENSER (R) or SI (Y) community or both (R/Y).

b. This attribute is defined in this ACP.

56. copyMember

a. The copyMember attribute value specifies a group of names associated with the object represented by the directory entry. In an Address List Ed. A directory entry, this attribute indicates the “copy” or “info” members of the list as opposed to “primary” or “action” members.

b. This attribute is defined in this ACP.

57. countryName

a. The countryName attribute value specifies a country. When used as a component of a directory name, it identifies the country in which the named object is physically located or with which it is associated in some other important way.

b. This attribute is defined in X.520.

58. crossCertificatePair

a. The forward elements of the crossCertificatePair attribute of a CA's directory entry shall be used to store all, except self-issued certificates issued to this CA. Optionally, the reverse elements of the crossCertificatePair attribute, of a CA's directory entry may contain a subset of certificates issued by this CA to other CAs. When both the forward and the reverse elements are present in a single attribute value, issuer name in one certificate shall match the subject name in the other and vice versa, and the subject public key in one certificate shall be capable of verifying the digital signature on the other certificate and vice versa.

b. When a reverse element is present, the forward element value and the reverse element value need not be stored in the same attribute value; in other words, they can be stored in either a single attribute value or two attribute values.

c. In the case of V3 certificates, none of the above CA certificates shall include a basicConstraints extension with the cA value set to FALSE.

d. The definition of realm is purely a matter of local policy.

e. This attribute is defined in X.509 (1997).

59. decUKMs

a. The decUKMs attribute value is used in the construction of selected CCEB symmetric confidentiality algorithms for the month of December.

b. This attribute is defined in this ACP.

60. deltaRevocationList

a. The deltaRevocationList attribute value is a partial certificateRevocationList (CRL) indicating only changes since the prior CRL issue.

b. This attribute is defined in X.509 (1997).

61. deployed

a. The deployed attribute value contains distinguished names of other directory entries that represent the same real world object in the field. See the garrison attribute.

b. This attribute is defined in this ACP.

62. description

a. The description attribute value specifies a text string which describes the associated object.

b. This attribute is defined in X.520.

63. destinationIndicator

a. The destinationIndicator attribute value specifies (in accordance with CCITT Recommendation F.1 and CCITT Recommendation F.31) the country and city associated with the object (the addressee) in order to provide the Public Telegram Service.

b. This attribute is defined in X.520.

64. distinguishedName

a. The distinguishedName attribute type is the attribute supertype from which attribute types, that specify the (directory) name of an object, are formed. The attributes in Common Content that are subtypes of distinguishedName are: administrator, aigsExpanded, deployed, garrison, guard, member, mhs-dl-related-lists, mhs-message-store-dn, owner, roleOccupant, and seeAlso.

b. This attribute is defined in X.520.

65. distributionCodeAction

a. The distributionCodeAction attribute values identify the distribution codes (including Subject Indicator Codes (SICs)) for which an organization, person, or role handles messages for action.

b. This attribute is defined in this ACP.

66. distributionCodeInfo

a. The distributionCodeInfo attribute values identify the distribution codes (including SICs) for which an organization, person, or role handles messages for information.

b. This attribute is defined in this ACP.

67. dnQualifier

a. The dnQualifier attribute value is used as part of a RDN to distinguish between directory entries for different objects..

b. This attribute is defined in X.520.

68. dualRoute

a. The dualRoute attribute value indicates whether delivery of messages for an organization to both the home and deployed sites is required. If set to TRUE, dual delivery is required.

b. This attribute is defined in this ACP.

69. effectiveDate

a. The effectiveDate attribute value indicates when the directory entry is to become valid.

b. This attribute is defined in this ACP.

70. enhancedSearchGuide

The enhancedSearchGuide attribute is defined in X.520, but is not used to meet Allied Directory requirements.

71. entryClassification

a. The entryClassification attribute value indicates the classification of the directory entry that contains this attribute. The possible values are: unmarked, unclassified, restricted, confidential, secret, and top secret.

b. This attribute is defined in this ACP.

72. expirationDate

a. The expirationDate attribute value indicates the time at which the directory entry becomes invalid.

b. This attribute is defined in this ACP.

73. facsimileTelephoneNumber

a. The facsimileTelephoneNumber attribute value specifies a telephone number for a facsimile terminal (and optionally its parameters) associated with the object represented by the directory entry.

b. An attribute value for the facsimileTelephoneNumber is a string that complies with the internationally agreed format for showing international telephone numbers, CCITT Recommendation E.123 (e.g., “+81 3 347 7418”) and an optional bit string (formatted according to CCITT Recommendation T.30).

c. This attribute is defined in X.520.

74. febUKMs

a. The febUKMs attribute value is used in the construction of selected CCEB symmetric confidentiality algorithms for the month of February.

b. This attribute is defined in this ACP.

75. garrison

a. The garrison attribute value contains distinguished names of other directory entries that represent the same real world object in garrison. See the deployed attribute.

b. This attribute is defined in this ACP.

76. gatewayType

a. The gatewayType attribute value is used to indicate the translations a messaging gateway is capable of performing. The translations that can be indicated are:

- acp120-acp127-gateway
- acp120-janap128-gateway
- acp120-mhs-gateway
- acp120-mmhs-gateway
- acp120-rfc822-gateway
- boundary MTA
- mmhs-mhs-gateway
- mmhs-rfc822-gateway
- mta-acp127-gateway

b. This attribute is defined in this ACP.

c. For the ACP120-acp127 translation, the messaging gateway performs the changes that are necessary to exchange messages between an acp120 organization and an acp127 organization.

77. generationQualifier

The generationQualifier attribute is defined in X.520, but is not used to meet Allied Directory requirements.

78. ghpType

a. The ghpType attribute value is used to indicate the gateway handling policy of an mta-acp127-gateway defined in STANAG 4406.

b. This attribute is defined in this ACP.

79. givenName

The givenName attribute is defined in X.520, but is not used to meet Allied Directory requirements.

80. guard

a. The guard attribute value indicates the Name(s) of the Guard Gateway.

b. This attribute is defined in this ACP.

81. host

a. The host attribute value gives an identifier for a host computer.

b. This attribute is defined in the COSINE and Internet X.500 Schema, RFC 1274.

82. hostOrgACP127

a. The hostOrgACP127 attribute value of a tenant PLA identifies the PLA for the organization which accepts traffic for a tenant.

b. This attribute is defined in this ACP.

83. houseIdentifier

The houseIdentifier attribute is defined in X.520, but is not used to meet Allied Directory requirements.

84. infoAddressees

a. The infoAddressees attribute value of an ACP 127/JANAP 128 collective contains the list of information addressees of the collective.

b. This attribute is defined in this ACP.

85. initials

The initials attribute is defined in X.520, but is not used to meet Allied Directory requirements.

86. internationalISDNNumber

a. The internationalISDNNumber attribute value specifies an International Integrated Services Digital Network (ISDN) Number associated with (the object represented by) the directory entry.

b. An attribute value for internationalISDNNumber is a string which complies with the internationally agreed format for ISDN addresses given in CCITT Recommendation E.164.

c. This attribute is defined in X.520.

87. janUKMs

a. The janUKMs attribute value is used in the construction of selected CCEB symmetric confidentiality algorithms for the month of January.

b. This attribute is defined in this ACP.

88. julUKMs

a. The julUKMs attribute value is used in the construction of selected CCEB symmetric confidentiality algorithms for the month of July.

b. This attribute is defined in this ACP.

89. junUKMs

a. The junUKMs attribute value is used in the construction of selected CCEB symmetric confidentiality algorithms for the month of June.

b. This attribute is defined in this ACP.

90. knowledgeInformation

a. The knowledgeInformation attribute value specifies a human readable description of knowledge mastered by a specific DSA.

b. This attribute is defined in X.520 but has been superseded by operational knowledge attributes defined in the 1993 edition of the standard. (See 196 b and 198 b in this annex.)

91. lastRecapDate

a. The lastRecapDate attribute value indicates when a list was last recapped or validated.

b. This attribute is defined in this ACP.

92. listPointer

a. The listPointer attribute value is used to point to Address List Ed. A directory entries which might have to be modified if the entry containing this attribute is modified. It is intended to be used to maintain data consistency in the DIB.

b. This attribute is defined in this ACP.

93. lmf

a. The lmf (Language and Media Format) attribute value indicates the language and media format that can be accepted between the two communicating end-systems. Possible values include:

- T tape
- A ASCII (American Standard Code for Information Interchange)
- C card, etc.

b. This attribute is defined in this ACP.

94. localityName

a. The localityName attribute value identifies a geographical area or locality in which the object represented by the directory entry is physically located or with which the object is associated in some other important way.

b. This attribute is defined in X.520.

95. longTitle

a. The longTitle attribute value is the expanded form of an organization's PLA.

b. This attribute is defined in this ACP.

96. mailDomains

a. The mailDomains attribute value is a string, which provides information on the domains that the messaging gateway will bridge.

b. This attribute is defined in this ACP.

97. marUKMs

a. The marUKMs attribute value is used in the construction of selected CCEB symmetric confidentiality algorithms for the month of March.

b. This attribute is defined in this ACP.

98. mayUKMs

a. The mayUKMs attribute value is used in the construction of selected CCEB symmetric confidentiality algorithms for the month of May.

b. This attribute is defined in this ACP.

99. member

a. The member attribute value specifies a group of names associated with the object represented by the directory entry. In an Address List Ed. A directory entry, this attribute indicates the “primary” or “action” members of the list as opposed to “copy” or “info” members.

b. This attribute is defined in X.520.

100. mhs-acceptable-eits

a. The mhs-acceptable-eits attribute value identifies a set of encoded information types (EITs) for messages. The user or distribution list, represented by the directory entry, will accept delivery of or expand a message in which any one of these EITs is present.

b. This attribute is defined in X.402.

101. mhs-deliverable-classes

a. The mhs-deliverable-classes attribute value identifies the classes of messages whose delivery a UA, represented by the directory entry, will accept.

b. This attribute is defined in X.402.

102. mhs-deliverable-content-types

a. The mhs-deliverable-content-types attribute values identify the content types of the messages whose delivery the user, represented by the directory entry, will accept.

b. This attribute is defined in X.402.

103. mhs-dl-archive-service

a. The mhs-dl-archive-service attribute value identifies a service from which a user may request copies of messages previously distributed by the address list represented by the directory entry.

b. This attribute is defined in X.402.

104. mhs-dl-members

a. The mhs-dl-members attribute value is an OR-name which identifies a member of the DL. This attribute may have multiple values each of which identifies one member of the DL. When a DL is expanded, each of the values of this attribute becomes a recipient of the message.

b. This attribute is defined in X.402.

105. mhs-dl-policy

a. The mhs-dl-policy attribute value identifies the choice of policy options to be applied when expanding the address list represented by the directory entry.

b. This attribute is defined in X.402.

106. mhs-dl-related-lists

a. The mhs-dl-related-lists attribute value identifies other address lists which are, in some unspecified way, related to the address list represented by the directory entry.

b. This attribute is defined in X.402.

107. mhs-dl-submit-permissions

a. The mhs-dl-submit-permissions attribute values identify the users and address lists that may submit messages to the address list represented by the directory entry.

b. This attribute is defined in X.402.

108. mhs-dl-subscription-service

a. The mhs-dl-subscription-service attribute value identifies a service of which a user may request changes to the membership of the address list represented by the directory entry, (e.g., for a user to request to be added to the address list).

b. This attribute is defined in X.402.

109. mhs-exclusively-acceptable-eits

a. The mhs-exclusively-acceptable-eits attribute value identifies a set of EITs for messages. The user or distribution list, represented by the directory entry, will accept delivery of or expand a message in which all of these EITs is present.

b. This attribute is defined in X.402.

110. mhs-maximum-content-length

a. The mhs-maximum-content-length attribute value identifies the maximum content length of the messages that can be handled by the object represented by the directory entry. The object is a user to whom the message would be delivered, an address list for which expansion would be performed on the message, or an MTA to which the message would be acceptable.

b. This attribute is defined in X.402.

111. mhs-message-store-dn

a. The mhs-message-store-dn attribute value identifies by directory name the message store of the user represented by the directory entry.

b. This attribute is defined in X.402.

112. mhs-or-addresses

a. The mhs-or-addresses attribute values specify the O/R addresses of the user or address list represented by the directory entry.

b. This attribute is defined in X.402.

113. mhs-or-addresses-with-capabilities

a. The mhs-or-addresses-with-capabilities attribute values specify the O/R addresses and the messaging capabilities associated with each address of the user or address list represented by the directory entry.

b. Recognized security labels are identified in ACP 123.

c. Information about availability and nationality will be included in the description. If the address is served by a foreign nation, the International Organization for Standardization 3166 code of the country shall be entered first.

d. If an OR-address is not operational on a 24 by 7 basis, the normal daily schedule shall be given in start and stop times for each day of operation. Planned down time also shall be given in start and stop time.

e. This attribute is defined in X.402.

114. mhs-supported-attributes

a. The mhs-supported-attributes attribute values identify the attributes the message store, represented by the directory entry, fully supports.

b. This attribute is defined in X.402.

115. mhs-supported-automatic-actions

a. The mhs-supported-automatic-actions attribute values identify the automatic actions that the message store, represented by the directory entry, supports.

b. This attribute is defined in X.402.

116. mhs-supported-content-types

a. The mhs-supported-content-types attribute values identify the content types of the messages whose syntax and semantics the message store, represented by the directory entry, supports.

b. This attribute is defined in X.402.

117. mhs-supported-matching-rules

a. The mhs-supported-matching-rules attribute values identify the matching rules the message store, represented by the directory entry, fully supports.

b. This attribute is defined in X.402.

118. mhs-unacceptable-eits

a. The mhs-undeliverable-eits attribute value identifies the encoded information types of a message which would make a user not accept delivery, or which would prevent an address list from doing expansion on the message. The absence of this attribute indicates that there are no EITs which are unacceptable. The presence of the special value “id-eit-all” indicates that all EITs are unacceptable except for those EITs identified by the mhs-acceptable-eits or mhs-exclusively-acceptable-eits attribute.

b. This attribute is defined in X.402.

119. militaryFacsimileNumber

a. The militaryFacsimileNumber attribute value identifies a military facsimile number, such as a Defense Switched Network (DSN) number or Defence Fixed Telecommunications Service (DFTS) number, which is associated with the object represented by the directory entry.

b. This attribute is a subtype of aCPTelephoneFaxNumber. An example of a militaryFacsimileNumber value is “DFTS, 555 1111 ext 25”.

c. This attribute is defined in this ACP.

120. militaryTelephoneNumber

a. The militaryTelephoneNumber attribute value identifies a military telephone number, such as a DSN number, which is associated with the object represented by the directory entry.

b. This attribute is a subtype of aCPTelephoneFaxNumber. An example of a militaryTelephoneNumber value is “DSN, 555-333”.

c. This attribute is defined in this ACP.

121. minimize

a. The minimize attribute value indicates whether an organization, person, or role, represented by the directory entry, is under the MINIMIZE condition. If so, the message originators are responsible for not sending unnecessary messages to the recipient.

b. This attribute is defined in this ACP.

c. Currently, the minimize attribute is not employed.

122. minimizeOverride

a. The minimizeOverride attribute value is used by the Message Conversion System (MCS) to determine whether the MINIMIZE condition will be enforced when a message is originated by this PLA. If the value is FALSE, override does not occur and MINIMIZE is enforced. If the value is TRUE, MINIMIZE is not enforced.

b. This attribute is defined in this ACP.

c. Currently, the minimizeOverride attribute is not employed.

123. name

a. The name attribute type is the attribute supertype from which string attribute types used for naming are formed. The attributes in Common Content that are subtypes of name are: commonName, surname, countryName, localityName, nationality, stateOrProvinceName, organizationName, organizationalUnitName, plaNameACP127, plasServed, and title.

b. This attribute is defined in X.520.

124. nameClassification

a. The nameClassification attribute value indicates the security classification of the name of the directory entry itself.

b. This attribute is defined in this ACP.

125. nationality

a. The nationality attribute value names the country which "owns" an entity. For an individual, it would be the nationality of the person. The standard Country Name attribute is used to denote the location of the entity.

b. This attribute is defined in this ACP.

126. networkDN

a. The networkDN attribute value contains the full DN of a network and may be used to reference the entry for the network from another entry (e.g., used in the Network Instructions Ed. B entry to reference the entry for the accessed network).

b. This attribute is defined in this ACP.

127. networkSchema

a. The networkSchema attribute value is a graphical representation of a network. It describes the structure of the network and details any rules associated with that network.

b. This attribute is defined in this ACP. Note that this attribute is replaced by the aCPNetworkSchemaEdB attribute.

128. novUKMs

a. The novUKMs attribute value is used in the construction of selected CCEB symmetric confidentiality algorithms for the month of November.

b. This attribute is defined in this ACP.

129. octUKMs

a. The octUKMs attribute value is used in the construction of selected CCEB symmetric confidentiality algorithms for the month of October.

b. This attribute is defined in this ACP.

130. onSupported

a. The onSupported attribute value indicates the types of notifications, besides MHS notifications, generated by an mta-acp127-gateway type of gateway. The gateway may generate all or none of the notifications. If the attribute is absent, the gateway does none of the notifications.

b. This attribute is defined in this ACP.

131. operationName

a. The operationName attribute value is the name of an official military operation. For example, when used in the definition of a network (i.e., in a Network directory entry), it could be the TURQUOISE operation which develops a RITA network.

b. This attribute is defined in this ACP.

132. organizationalUnitName

a. The organizationalUnitName attribute value specifies an organizational unit. When used as a component of a directory name, it identifies an organizational unit with which the named directory entry is affiliated. The designated organizational unit is understood to be part of an organization designated by an organizationName attribute value. It follows that, if an organizationalUnitName attribute value is used in a directory name, it must be associated with an organizationName attribute value.

b. An attribute value for organizationalUnitName is a string chosen by the organization of which it is part (e.g., OU = “Technology Division”). Note that the commonly used abbreviation “TD” would be a separate and alternative attribute value. Example: O = “Scottel”, OU = “TD”.

c. This attribute is defined in X.520.

133. organizationName

a. The organizationName attribute type value identifies an organization. When used as a component of a directory name, it identifies an organization with which the named directory entry is affiliated.

b. An attribute value for organizationName is a string chosen by the organization (e.g. O = “Scottish Telecommunications plc”). Any variants should be associated with the named organization as separate and additional attribute values.

c. This attribute is defined in X.520.

134. owner

a. The owner attribute value specifies the name of some object which has some responsibility for the directory entry that contains this attribute. An attribute value for owner is a distinguished name (which could represent a group of names) and can have several values.

b. This attribute is defined in X.520.

135. physicalDeliveryOfficeName

a. The physicalDeliveryOfficeName attribute value specifies the name of the city, village, etc. where the physical delivery office, that serves the object represented by the directory entry, is situated. An attribute value for physicalDeliveryOfficeName is a string.

b. This attribute is defined in X.520.

136. plaAddressees

a. The plaAddressees attribute value of an ACP 127/JANAP 128 collective contains the list of action and information addressees of the collective. It is used for some types of collectives instead of separating action and information addressees.

b. This attribute is defined in this ACP.

137. plaNameACP127

a. The plaNameACP127 attribute value is the object's (represented by the directory entry) ACP 127/JANAP 128 plain language address. A PLA is sometimes called the Signal Message Address or registered PLA. The long form of the PLA name is represented in the ACP 133 by the longTitle attribute.

b. This attribute is defined in this ACP.

138. plaReplace

a. The plaReplace attribute value is used by ACP 127/JANAP 128. When an "alternate spelling" PLA is addressed on a message, the MCS will look at the value of this attribute in the PLA's directory entry. If set, the alternate spelling on the message will be replaced with the "primary" or correct spelling. (Each alternate spelling has a pointer to the primary PLA.)

b. This attribute is defined in this ACP.

139. plasServed

a. The plasServed attribute value is a list of the PLAs accessible through a gateway.

b. This attribute is defined in this ACP.

140. positionNumber

a. The position number attribute value is used by government and Defense agencies to identify uniquely each individual's position, and possibly role and duties, within the organization.

b. This attribute is defined in this ACP.

141. postalAddress

a. The postalAddress attribute value is the address information required for the physical delivery of postal messages by the postal authority to the object represented by the directory entry. An attribute value for Postal Address will typically be composed of selected attributes from the MHS Unformatted Postal O/R Address version 1 according to CCITT Recommendation F.401 and limited to 6 lines of 30 characters each, including a Postal Country Name. Normally, the information contained in such an address could include an addressee's name, street address,

city, state or province, postal code and possibly a Post Office Box number depending on the specific requirements of the object.

b. This attribute is defined in X.520.

142. postalCode

a. The postalCode attribute value specifies the postal code of the object represented by the directory entry. If this attribute value is present it will be part of the object's postal address.

b. This attribute is defined in X.520.

143. postOfficeBox

a. The postOfficeBox attribute value is the identifier of the Post Office Box at which the object, represented by the directory entry, receives physical postal delivery. If present, the attribute value is part of the object's postal address.

b. This attribute is defined in X.520.

144. preferredDeliveryMethod

a. The preferredDeliveryMethod attribute value indicates the priority order regarding the method to be used for communicating with the object represented by the directory entry. The possible methods that may be indicated in a value of this attribute are:

- any-delivery-method,
- mhs-delivery,
- physical-delivery,
- telex-delivery,
- teletex-delivery,
- g3-facsimile-delivery,
- g4-facsimile-delivery,
- ia5-terminal-delivery,
- videotex-delivery,
- telephone-delivery

b. This attribute is defined in X.520.

145. presentationAddress

a. The presentationAddress attribute value specifies a presentation address associated with an application entity object, represented by the directory entry.

b. This attribute is defined in X.520.

146. primarySpellingACP127

a. The primarySpellingACP127 attribute value of an Alternate Spelling PLA directory entry is the object's correct PLA spelling.

b. This attribute is defined in this ACP.

147. proprietaryMailboxes

a. The proprietaryMailboxes attribute value identifies a mail box identifier that can be used to address mail within the local proprietary domain, such as cc:mail.

b. This attribute is defined in this ACP.

148. protocolInformation

a. The protocolInformation attribute value indicates the associated protocol information for each network address in the presentationAddress attribute.

b. This attribute is defined in X.520.

149. publish

a. The publish attribute value indicates whether this PLA should be published in the Message Address Directory or the ACP 117. Access controls may be set based on this attribute.

b. This attribute is defined in this ACP.

150. rank

a. The value of the rank attribute type contains the military or civilian rank of an individual such as Major or civilian grade.

b. This attribute is defined in this ACP.

151. recapDueDate

a. The recapDueDate attribute value indicates when a list is expected to be recapped or validated.

b. This attribute is defined in this ACP.

152. registeredAddress

a. The registeredAddress attribute value is a mnemonic for an address associated with an object at a particular city location. The mnemonic is registered in the country in which the city is located and is used in the provision of the Public Telegram Service (according to CCITT Recommendation F.1).

b. This attribute is defined in X.520.

153. releaseAuthorityName

a. The releaseAuthorityName attribute value is a relative distinguished name of a release authority for an organization.

b. This attribute is defined in this ACP.

154. remarks

a. The remarks attribute value is textual information associated with a PLA's directory entry. These remarks may be instructions rather than a description of the entity.

b. This attribute is defined in this ACP.

155. rfc822Mailbox

a. The rfc822Mailbox attribute value is an electronic mailbox identifier following the syntax in RFC 822. An example for a user on a military network is "user@host.Service.mil".

b. This attribute is defined in the COSINE/Internet schema, RFC 1274.

156. rI

a. The rI (Routing Indicator) attribute value is the information mapped to in ACP 127/JANAP 128 from a user's PLA name. Users are named by their PLA names and delivered to by their routing indicator values, analogous to Directory Names and O/R Addresses for X.400 users.

b. This attribute is defined in this ACP.

157. rIClassification

a. The rIClassification attribute value indicates the highest classification of data allowed to be processed by a specified device.

b. This attribute is defined in this ACP.

158. rIInfo

a. The rIInfo attribute value is RI values with the associated properties of each RI.

b. This attribute is defined in this ACP.

159. roleOccupant

a. The roleOccupant attribute value is the distinguished name of a directory entry that represents the person or organizational unit who fulfills an organizational role.

b. This attribute is defined in X.520.

160. roomNumber

a. The roomNumber attribute value identifies a room number.

b. This attribute is defined in the COSINE/Internet schema, RFC 1274.

161. searchGuide

a. The searchGuide attribute value specifies suggested search criteria which may be included in some entries expected to be convenient base-objects for search operations, e.g., Country or Organization.

b. Search criteria consist of an optional identifier for the type of object sought and combinations of attribute types and logical operators to be used in the construction of a filter. It is possible to specify for each search criteria item the matching level, e.g., approximate match.

c. The searchGuide attribute value may have multiple values to reflect the various types of requests, e.g., search for a Residential Person or an Organizational Person, which may be fulfilled from the directory entry where the Search Guide is read.

d. This attribute is defined in X.520.

162. secondPartyAddressees

a. The secondPartyAddressees attribute value is a list of second party action PLAs.

b. This attribute is defined in this ACP.

163. section

a. The section attribute value is set to TRUE if the receiving PLA requires message sectioning to be performed. This is required to transition users with slow-speed terminals.

b. This attribute is defined in this ACP.

164. secureFacsimileNumber

a. The secureFacsimileNumber attribute value is a facsimile number that is used for secure communication with the object represented by the directory entry.

b. This attribute is a subtype of aCPTelephoneFaxNumber. An example of a secureFacsimileNumber value is “DSN, 555-333”.

c. This attribute is defined in this ACP.

165. secureTelephoneNumber

a. The secureTelephoneNumber attribute value is a telephone number of a secure device, such as STU II or STU III, that is used for secure communication with the object represented by the directory entry.

b. This attribute is a subtype of aCPTelephoneFaxNumber. An example of a secureTelephoneNumber value is “PSTN, +1 555 222, STU III”.

c. This attribute is defined in this ACP.

166. seeAlso

a. The seeAlso attribute value contains distinguished names of other directory entries which may be other aspects (in some sense) of the same real world object. For example, an Organizational Person Ed. B directory entry may include the distinguished names of the Organizational Role Ed. B directory entries which designate the organizational person as a role occupant. See paragraph 310 in Chapter 3 of this ACP.

b. This attribute is defined in X.520.

167. sepUKMs

a. The sepUKMs attribute value is used in the construction of selected CCEB symmetric confidentiality algorithms for the month of September.

b. This attribute is defined in this ACP.

168. serialNumber

a. The serialNumber attribute value specifies an identifier, the serial number, of a device.

b. This attribute is defined in X.520.

169. serviceNumber

a. The serviceNumber attribute value is the staff identifier number used by government and defense agencies for purposes such as payroll references, medical records, human resources, and duty rosters.

b. This attribute is defined in this ACP.

170. serviceOrAgency

a. The serviceOrAgency attribute value is an identifier of the Service or agency to which the PLA belongs.

b. This attribute is defined in this ACP.

171. sHD

a. The sHD (specialHandlingDesignator) attribute value is a string containing the special handling designator which an entity, address, or routing indicator can support.

b. This attribute is defined in this ACP.

172. shortTitle

a. The shortTitle attribute value is a PLA name used for Signal Intelligence (SIGINT) related communications.

b. This attribute is defined in this ACP.

173. sigad

a. The sigad (SIGINT Address) attribute value is a PLA name used for sensitive SIGINT related communications.

b. This attribute is defined in this ACP.

174. spot

a. The spot attribute value identifies a special project address list or collective.

b. This attribute is defined in this ACP.

175. stateOrProvinceName

a. The stateOrProvinceName attribute value indicates a state or province. When used as a component of a directory name, it identifies a geographical subdivision in which the object, represented by the directory entry, is physically located or with which the object is associated in some other important way.

b. This attribute is defined in X.520.

176. streetAddress

a. The streetAddress attribute value specifies a site for the local distribution and physical delivery in a postal address, i.e., the street name, place, avenue, and house number. When used as a component of a directory name, it identifies the street address at which the

object, represented by the directory entry, is located or with which the object is associated in some other important way.

b. This attribute is defined in X.520.

177. supportedAlgorithms

a. The supportedAlgorithms attribute value is used to list the algorithms supported by the user.

b. This attribute is defined in X.509.

178. supportedApplicationContext

a. The supportedApplicationContext attribute value is the object identifier(s) of an application context(s) that the object (an OSI application entity) supports.

b. This attribute is defined in X.520.

179. surname

a. The surname attribute value is the linguistic construct which normally is inherited by an individual from the individual's parent or assumed by marriage, and by which the individual is commonly known.

b. This attribute is defined in X.520.

180. tARE

a. The tARE (Telegraph Automatic Relay Equipment) attribute value is a flag that specifies delivery responsibility for a message that is received by an intermediary. The flag is set in the directory entry for the intended recipient.

b. This attribute is defined in this ACP.

181. tCC

a. The tCC (Transmission Control Code) attribute value specifies a message handling instruction used in the routing indicator.

b. This attribute is defined in this ACP.

182. tCCG

a. The tCCG (Transmission Control Code Group) attribute value specifies a group of message handling instructions used in the routing indicator.

b. This attribute is defined in this ACP.

183. telephoneNumber

a. The telephoneNumber attribute value specifies a number for a telephone (and optionally its parameters) associated with the object represented by the directory entry.

b. An attribute value for telephoneNumber is a string that complies with the internationally agreed format for showing international telephone numbers, CCITT Recommendations E.123 (e.g., "+44 582 10101").

c. An extension should be indicated by writing the nationally used word or abbreviation for "extension" immediately after the telephone number, followed by the extension number itself. For example: "+22 607 123 4567 ext. 876."

d. This attribute is defined in X.520.

184. teletexTerminalIdentifier

a. The teletexTerminalIdentifier attribute value is the Teletex terminal identifier (and, optionally, parameters) for a teletex terminal associated with the object represented by the directory entry.

b. An attribute value for teletexTerminalIdentifier is a string which complies with CCITT recommendation F.200 and an optional set whose components are determined according to CCITT recommendation T.62.

c. This attribute is defined in X.520.

185. telexNumber

a. The telexNumber attribute value is the telex number, country code, and answerback code of a telex terminal associated with the object represented by the directory entry.

b. This attribute is defined in X.520.

186. title

a. The title attribute value is the designated position or function of the object, represented by the directory entry, within an organization, e.g., Company Clerk.

b. This attribute is defined in X.520.

187. transferStation

a. The transferStation attribute value indicates whether a message for the entity should be sent to a communications processing and routing system, called a transfer station. For example, a Naval Communications Processing and Routing System (NAVCOMPARS) is a transfer station. If this attribute is TRUE, traffic should be routed to a transfer station.

b. This attribute is defined in this ACP.

188. tRC

a. The tRC (Transmission Release Code) attribute value is the classification of data used in the routing indicator. Possible values include:

- A Australia
- B British Commonwealth less Canada, Australia, and New Zealand
- C Canada
- U US
- X Belgium, Denmark, France, Germany, Greece, Italy, Netherlands, Norway, Portugal, Turkey, NATO
- Z New Zealand

b. This attribute is defined in this ACP.

189. uniqueIdentifier

The uniqueIdentifier attribute is defined in X.520, but is not used to meet Allied Directory requirements.

190. uniqueMember

The uniqueMember attribute is defined in X.520, but is not used to meet Allied Directory requirements.

191. usdConversion

a. The usdConversion attribute value is an organizational address that is used when other types of address are not appropriate.

b. This attribute is defined in this ACP.

192. userCertificate

a. The userCertificate attribute contains the public keys of a user, together with some other information, rendered unforgeable by encipherment with the private key of the certification of the certification authority that issued it.

b. This attribute is defined in X.509.

193. userPassword

a. A userPassword attribute value is the password used for simple authentication of the object represented by the directory entry.

b. This attribute is defined in X.509.

194. x121Address

a. The X.121 Address attribute value is an address, as defined by ITU-T Recommendation X.121, that is associated with the object represented by the directory entry.

b. This attribute is defined in X.520.

195. Useful

The following paragraphs define attributes that may be useful, but are not part of the Common Content.

a. hoursOfOperation

(1) A value of the hoursOfOperation attribute contains the scheduled hours of operation of an organizational unit.

(2) This attribute is defined in this ACP.

b. jpegPhoto

(1) A value of the jpegPhoto attribute is a JPEG image in the JPEG File Interchange Format (JFIF).

(2) This attribute is defined in the inetOrgPerson Internet-Draft..

c. militaryPostalAddress

(1) A value of the militaryPostalAddress attribute is an address assigned by a military authority and used by military postal services.

(2) This attribute is defined in this ACP.

d. visitorAddress

(1) A value of the visitorAddress attribute describes an address for visitors who want to access a site. It may also be used if the postal address is different from the physical address.

(2) This attribute is defined in this ACP.

SECTION X

DIRECTORY SYSTEM SCHEMA

196. General

a. This subsection lists the information required for the Directory to know how to operate correctly. It specifies the type of information that is required in the Directory System Schema. The Directory System Schema consists of:

- definition of subentry object classes
- definition of Directory operational attributes

b. The Directory System Schema is distributed. Each administrative authority establishes the part of the system schema that will apply for those portions of the DIB administered by the authority. Each DSA participating in a directory system requires a full knowledge of the system schema established by its administrative authority. The Directory System Schema is not regulated by DIT structure or content rules and is normally viewed and controlled by the Directory Administrator or the DSA itself.

197. Standard Subentry Object Classes

The following subentry object classes are defined by X.501 and shall be supported by the ACP 133 Directory.

a. The subentry object class supports the Administrative and Operational Information Model of the Directory. The subentry object class is used to define the name and subtree for an access control, collective attribute, or subschema subentry of an administrative point.

b. The accessControlSubentry object class contains precisely one prescriptive Access Control Information attribute which contains access control information applicable to directory entries within that subentry's scope.

c. The collectiveAttributeSubentry shall contain at least one collective attribute which is available for interrogation and filtering at every entry within the scope of the subentry's Subtree Specification attribute.

d. The subschema object class is used to contain the operational attributes that represent the policy parameters used to express subschema policies (schema publication). The attributes include the rules and constraints concerning DIT structure, DIT content, object classes and attribute types, syntaxes, and matching rules which characterize the DIB.

198. Standard Operational Attributes

Operational attributes defined by X.500 and cited in this paragraph shall be supported by the ACP 133 Directory. The definition of an operational attribute includes a specification of the way in which the Directory uses and manages the attribute in the course of its operation. There

are two varieties of operational attribute: Directory operational attributes and DSA Specific Entry (DSE) operational attributes. Directory operational attributes occur in the Directory information model and are used to represent control information or other information provided by the Directory. DSE operational attributes are further categorized into two: DSA-shared operational attribute and DSA-specific operational attribute. They occur only in the DSA information model and are not visible at all in the Directory Information model.

a. Directory Operational Attributes

(1) The subtreeSpecification attribute shall be supported by the ACP 133 Directory. It supports the administrative and operational information model and is used to specify the scope of a subentry or area of replication. It is also used to regulate the subentries permitted to be subordinate to an administrative entry such as access control or collective attribute subentries.

(2) The administrativeRole attribute shall be supported by the ACP 133 Directory. It supports the administrative model and is used to indicate the role or roles of an administrative entry. The attribute may be stored in one or more of the following administrative points:

- Autonomous Administrative Point
- Access Control Administrative Point
- Access Control Inner Administrative Point
- Subschema Administrative Point
- Collective Attribute Administrative Point
- Collective Attribute Inner Administrative Point

(3) The attributes below, which may be contained in an entry or subentry, support general administrative and operational requirements. These attributes shall be supported by the ACP 133 Directory. All DSAs which conform to this ACP shall automatically provide date/time of creation/modification and creators/modifiers name on directory add and modify operations. Replication requires the use of createTimestamp and modifyTimestamp. The creatorsName and modifiersName are desirable for audit purposes.

- createTimestamp
- modifyTimestamp
- creatorsName
- modifiersName

(4) The collectiveExclusions attribute allows particular collective attributes to be excluded from an entry and shall be supported.

(5) The following attributes are used by the Security Model of the Directory and shall be supported:

- accessControlScheme,
- prescriptiveACI (Basic or Simplified Access Control),
- entryACI (Basic Access Control),
- subentryACI (Basic or Simplified Access Control)

(6) The accessControlScheme indicates which access control model, such as, Basic Access Control or Simplified Access Control, is in effect for an administrative area. It is placed in the Administrative Entry for the corresponding Administrative Point. The prescriptiveACI attribute is contained in an access control subentry. The entryACI, which may be used in Basic Access Control, is an operational attribute of an entry or subentry and contains access control information applicable to that entry. The subentryACI attribute is used in an administrative entry to provide access control information for subentries of the administrative point.

b. DSA Specific Entry (DSE) Operational Attributes

(1) Each directory entry in the DSA also contains additional attributes beyond what are visible to Directory administrator. The following attributes are operational attributes contained in DSEs. These attributes are used by the DSA Information Model and shall be supported by the ACP 133 Directory:

- dseType
- myAccessPoint
- superiorKnowledge
- specificKnowledge
- nonSpecificKnowledge
- supplierKnowledge
- consumerKnowledge
- secondaryShadows

(2) The dseType indicates the role or roles of a DSE, such as entry, subentry, or administrative point. The myAccessPoint attribute is an operational attribute used to represent its own access point and is contained in the root DSE. The information may be used by the DOP when establishing or modifying an operational binding. The superior, specific, and non-specific knowledge attributes are used by the DSA to find access points of DSAs for a naming context. The supplierKnowledge and consumerKnowledge attributes are used by the DSA to know the

access points and shadowing agreement identifiers of a replicated area. They are managed by the DSA itself. The secondaryShadows attribute is managed by the DSA itself and contains access points of consumer DSAs which are engaged in secondary shadowing.

(3) A DSE may have only the user attributes, the operational attributes or both depending on its role within the total DIB. Therefore, to identify an entry with its role and DIB location and its effect in the scheme of the total (and possibly distributed and replicated) DIB, a number of DSE entry types have been defined. Table B-50 defines the standard DSE types and their purpose. The DSE types shall be supported by this ACP for all DSAs in accordance with their definition.

Table B-55
DSE Types and Their Purpose

DSE Type	Purpose
root	Is the root of the DSA Information Tree.
glue	Represents knowledge of a name only. Used to connect the fragments of a DIT in shadowed copies, for example.
cp	Is the context prefix of a naming context, the root of a subtree.
entry	Holds an object entry, user information.
alias	Holds an alias entry.
subr	Holds a reference to a DSA holding a portion of the DIT subordinate to that in this DSA. Contains the context prefix of the subordinate.
nssr	Holds a non-specific subordinate reference to a DSA that holds some subordinate that is not named.
supr	Holds a superior reference, a DSA which holds a naming context superior in the DIT to all the naming contexts held by this DSA.
xr	Holds a cross reference to another DSA, used for optimization. Points directly to a remote naming context.
admpoint	Is an administrative point, the root vertex of an administrative area, a subtree of the DIT whose entries are all administered by the same Administrative Authority.
subentry	A subentry that is located under an administrative point and contains policy for access control, schema, and collective attributes.
shadow	Holds a shadow copy of an entry or part of an entry. Set by the shadow consumer.
immSupr	Holds a reference to a naming context immediately superior to the referencing one.
rhob	Holds information about a superior administrative point or subentry passed by a Relevant Hierarchical Operational Binding between DSAs.
sa	Subordinate reference DSE points to an alias entry.

199. Rules for DIT Schema Management

The following attributes specify the subschema policy and are contained in the subschema subentry and shall be supported:

- dITContentRules
- dITStructureRules
- matchingRules
- attributeTypes
- objectClasses
- nameForms
- matchingRuleUse
- structuralObjectClass
- governingStructureRule

SECTION XI

NATIONAL DIRECTORY INFORMATION TREES

200. Australian DIT

Figure B-3 shows the military portion of the Australian DIT from the top through the first level within the military subtree and the first level of the Army subtree. The remaining subtrees and levels of the military subtree will be shown in the future.

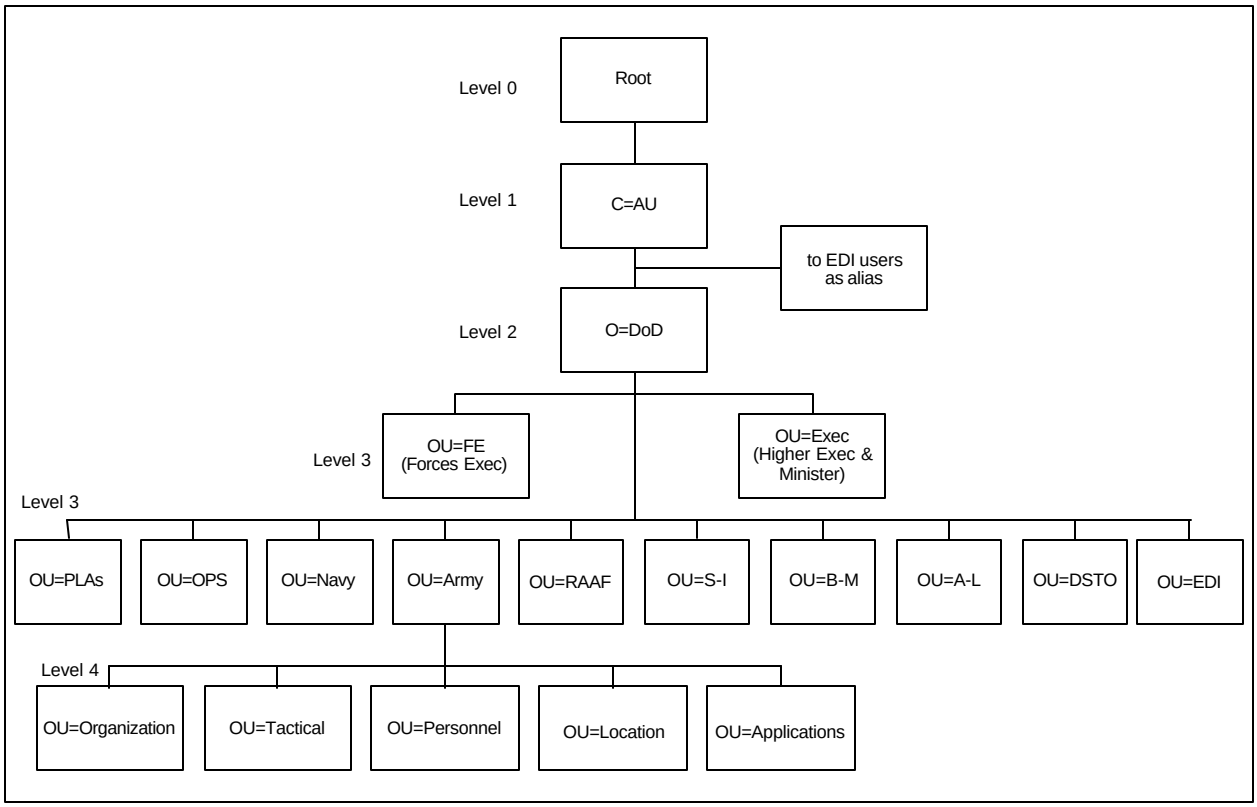

Figure B-3
Australian Top-Level DIT

201. Canadian DIT

Figure B-4 shows the military portion of the Canadian DIT from the top through the beginning of the two military subtrees. The remaining levels of the military subtrees will be shown in the future.

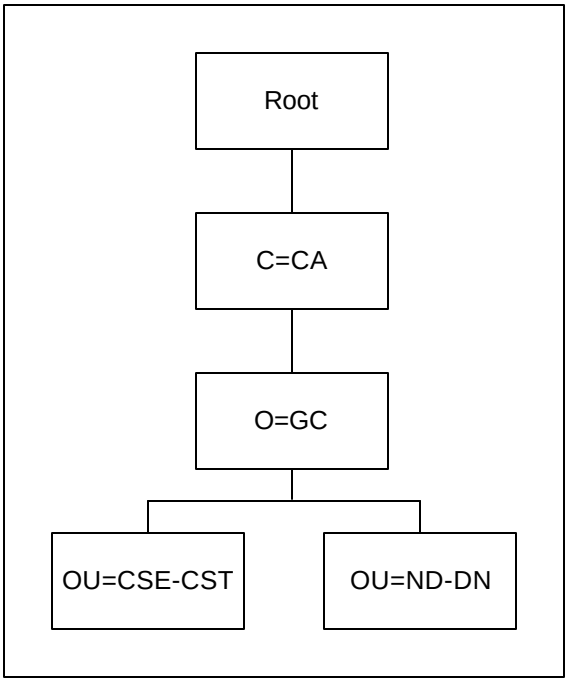

Figure B-4
Canadian Top-Level DIT

202. New Zealand DIT

Figure B-5 shows the military portion of the New Zealand's DIT from the top through the beginning of the (two) military subtrees. The remaining levels of the military subtrees will be shown in the future.

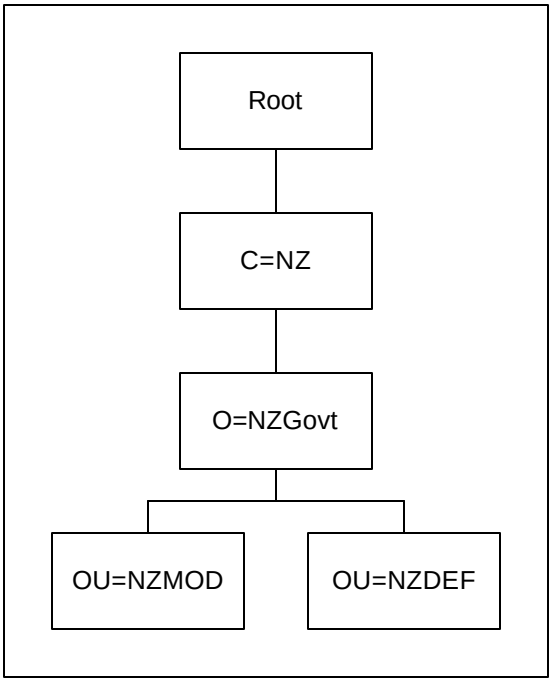

Figure B-5
New Zealand Top-Level DIT

203. United Kingdom DIT

Figure B-6 shows the military portion of the United Kingdom's DIT from the top through the first level within the military subtree. The remaining levels of the military subtree will be shown in the future.

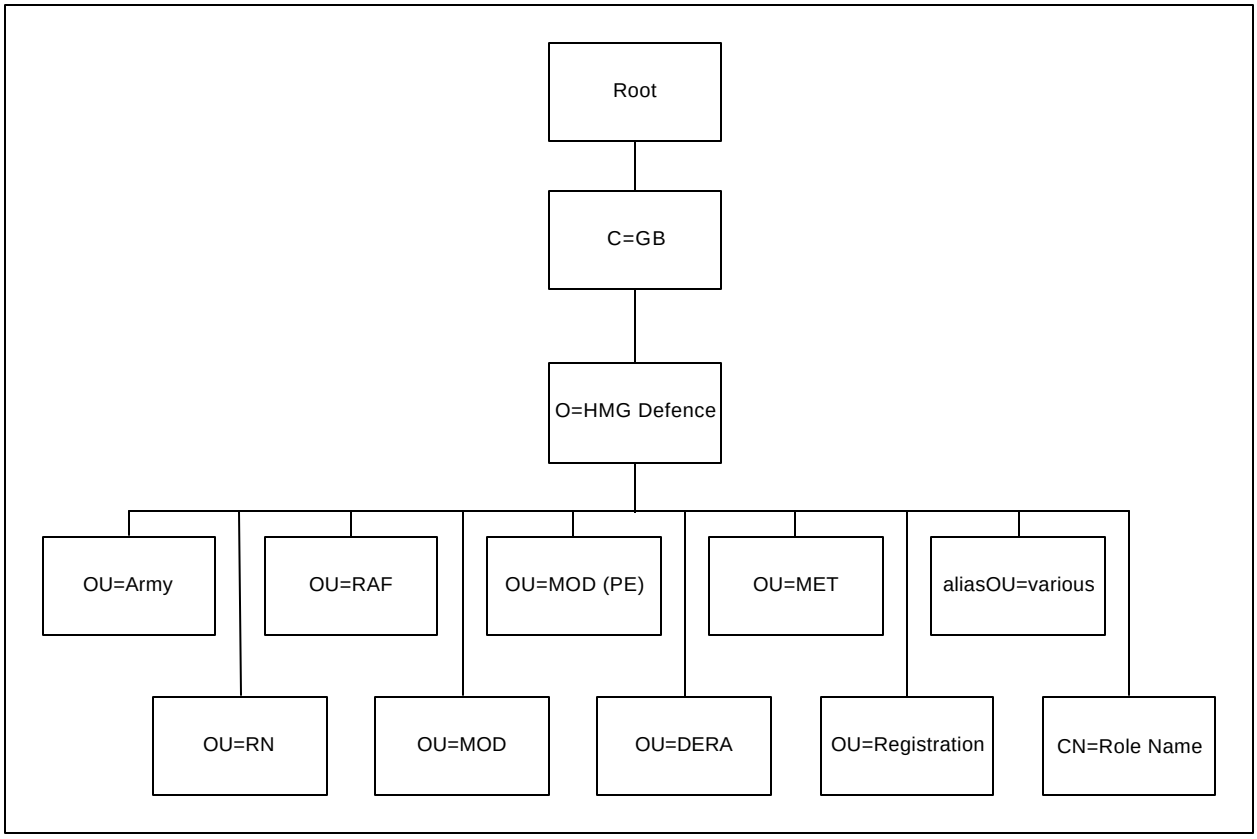

Figure B-6
UK Top-Level DIT

204. United States DIT

a. Top-Level

Figure B-7 shows the military portion of the United States' DIT from the top through the first level within the military subtree. In the U.S. DIT, the military is represented by an Organizational Unit Ed. B directory (OU=DoD) entry under the Organization Ed. B directory entry that represents the U.S. government. The DoD level is followed by a level that contains an Organizational Unit Ed. B directory entry for each Service, agency, and command.

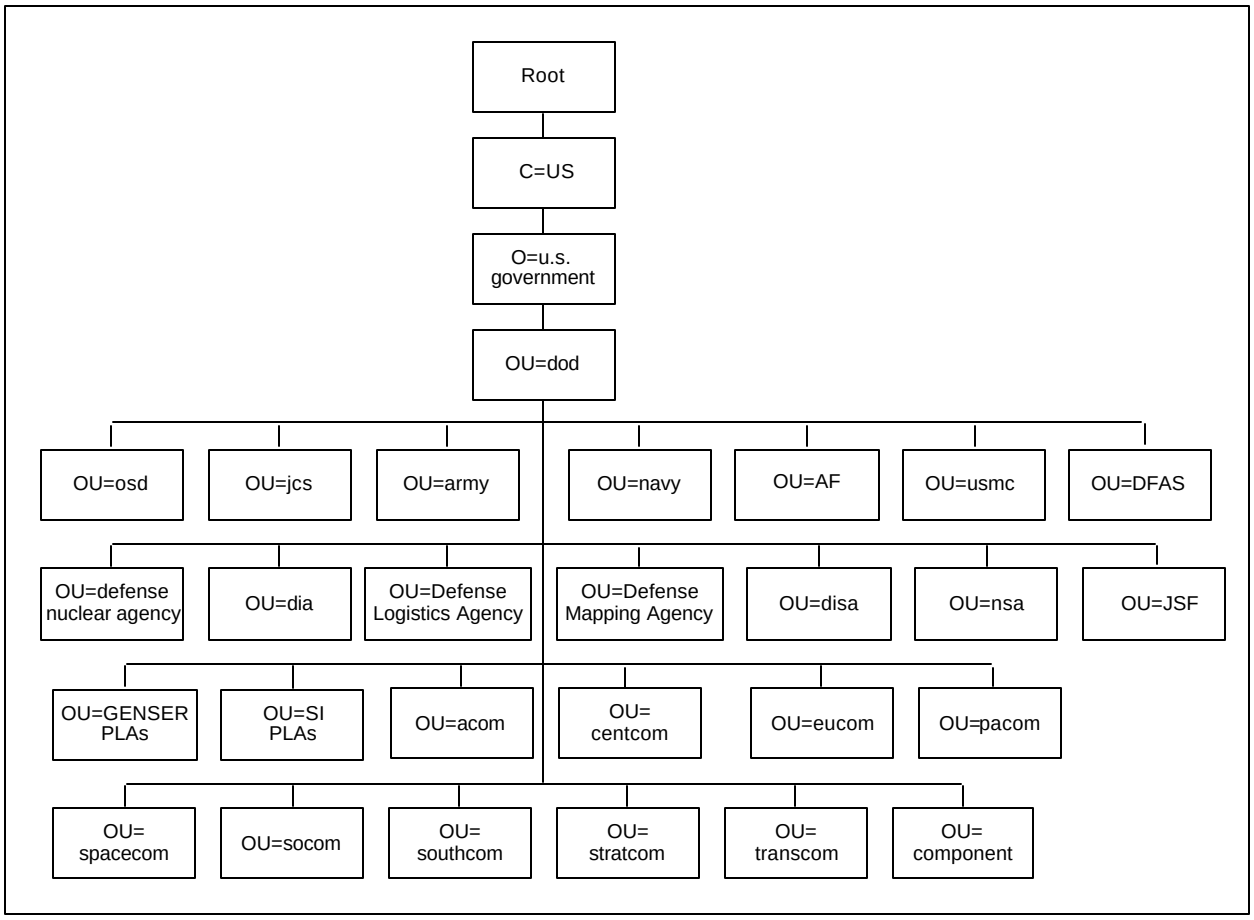

Figure B-7
U.S. Top-Level DIT

b. Service/Agency/Command Subtrees

Under each Service/agency/command directory entry there are at least two subtrees, one for locations, one for organizations, and up to three for special uses appropriate for the

Service/agency/command: ships, address lists, and tactical users. This level is shown in Figure B-8.

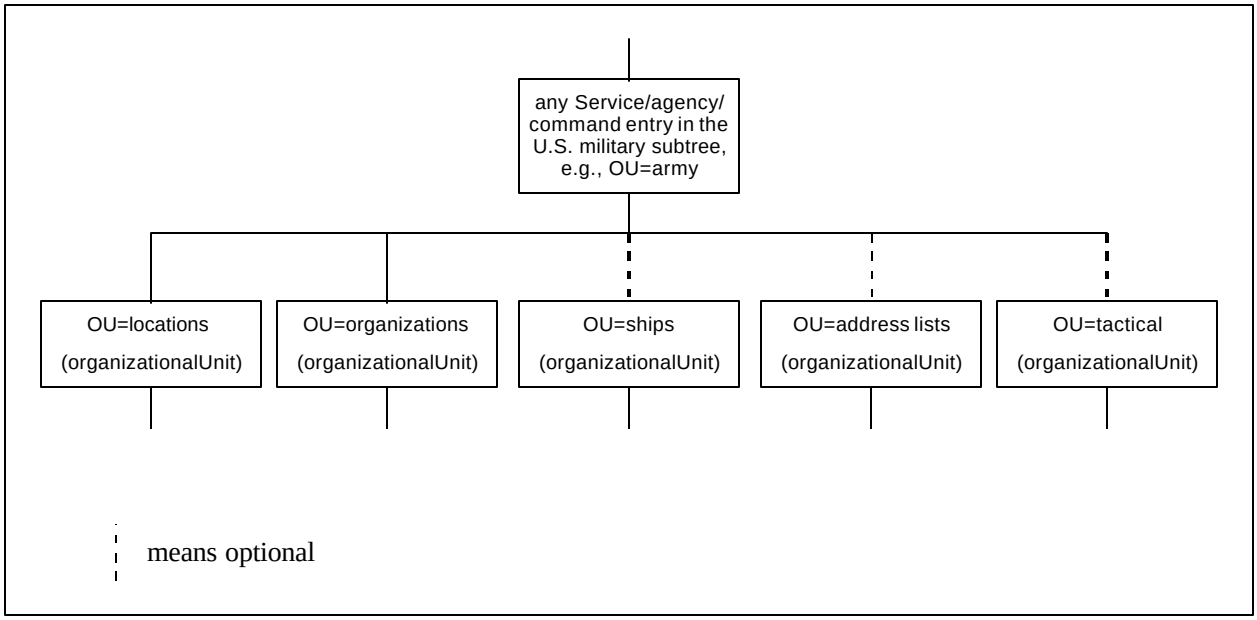

Figure B-8
U.S. DIT Subtrees for Each Service/Agency/Command

(1) Generally, organizational persons will be listed in the locations subtree, shown in Figure B-9, and organizational roles, release authorities, and address lists will be listed in the organizations subtree, shown in Figure B-10. An exception is the role of certification authority which will appear in both locations and organizations subtrees. Aliases for organizational roles may be listed in the locations subtree, and aliases for organizational persons may be listed in the organizational subtree. Devices and application entities may be located in any location or organizational subtree, as appropriate. In the locations subtree, note the optional level of organizational unit. This is used to segment the DIB across multiple DSAs at a site. The organizational subtree also provides for subdivision into localities, if desired.

(2) Figure B-11 and Figure B-12 give examples of the directory entries that could be present in an instance of the locations and organizations subtrees under the Army. Figure B-13 gives examples of the directory entries that could be present in an instance of the locations and organizations subtrees for a combined task force under the Pacific Command (PACOM).

(3) From Figure B-11 and Figure B-12, example Distinguished Names for an individual, a release authority for an organization, and a position in an organization are, respectively:

- { C=US, O=u.s. government, OU=dod, OU=army, OU=locations, L=Fort Huachuca AZ, OU=USAISC, CN=Jones, James R. },
- { C=US, O=u.s. government, OU=dod, OU=army, OU=organizations, OU=DISC4, OU=USAISEC, OU=ASOP-OI, RAN=Jones, James R. }, and
- { C=US, O=u.s. government, OU=dod, OU=army, OU=organizations, OU=DISC4, OU=USAISEC, OU=ASOP-OI, CN=security officer }

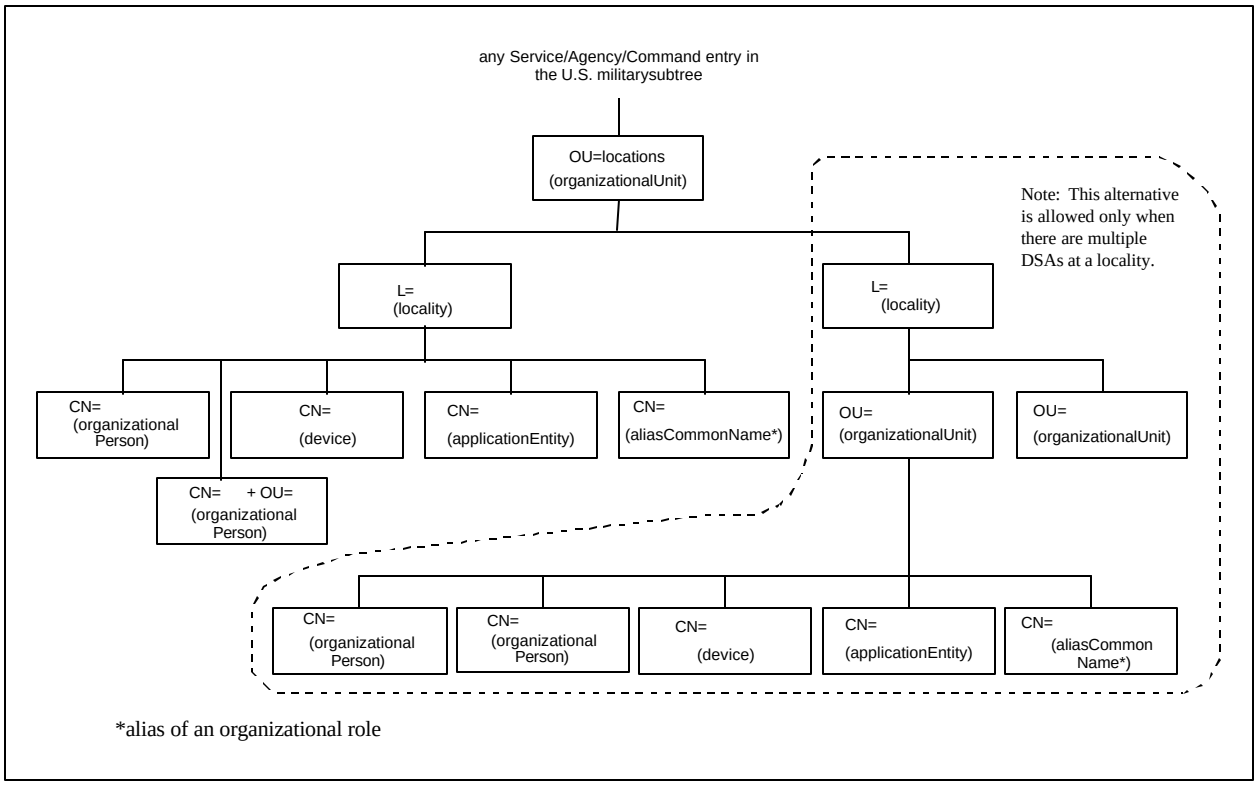

Figure B-9
U.S. DIT Locations Subtree

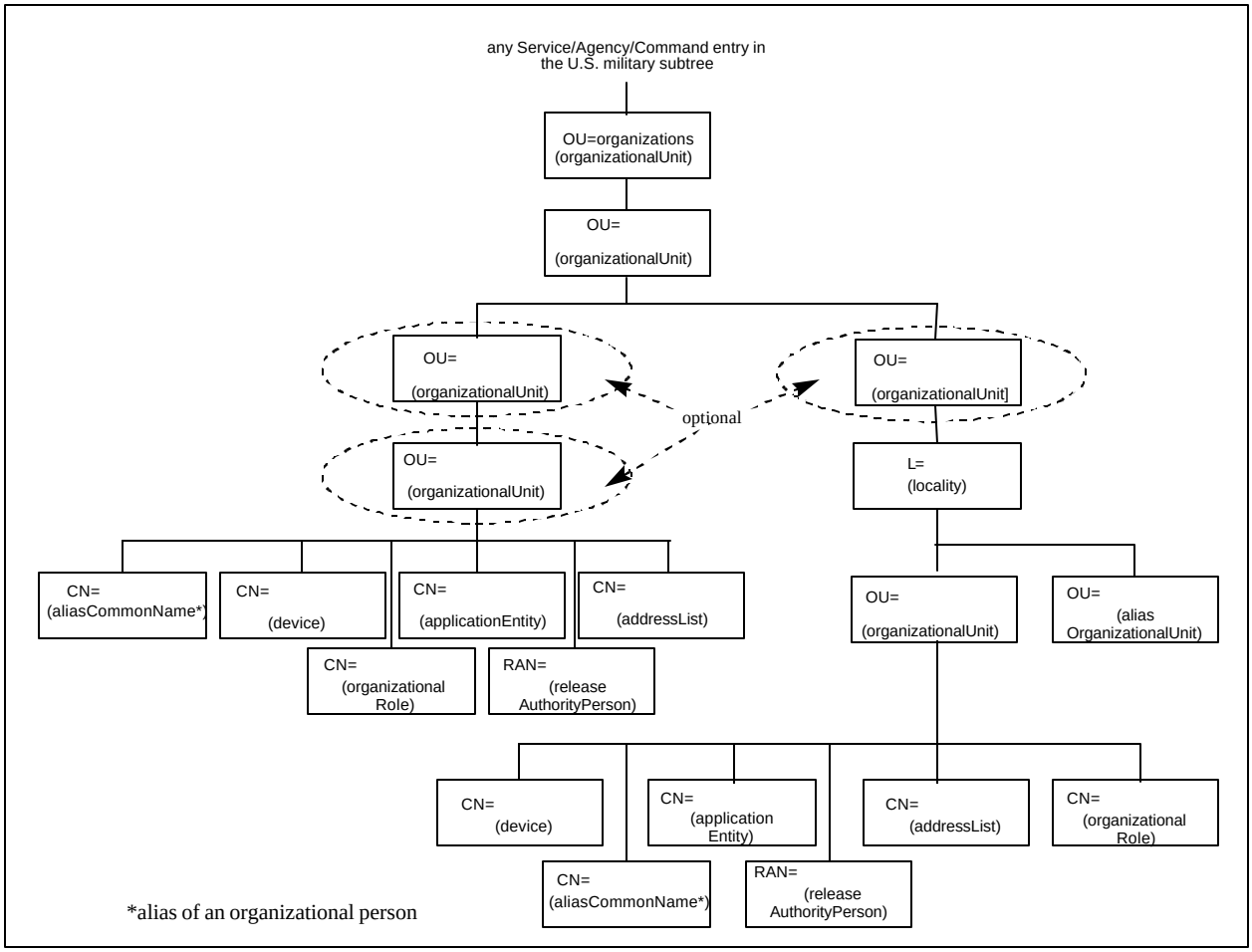

Figure B-10
U.S. DIT Organizations Subtree

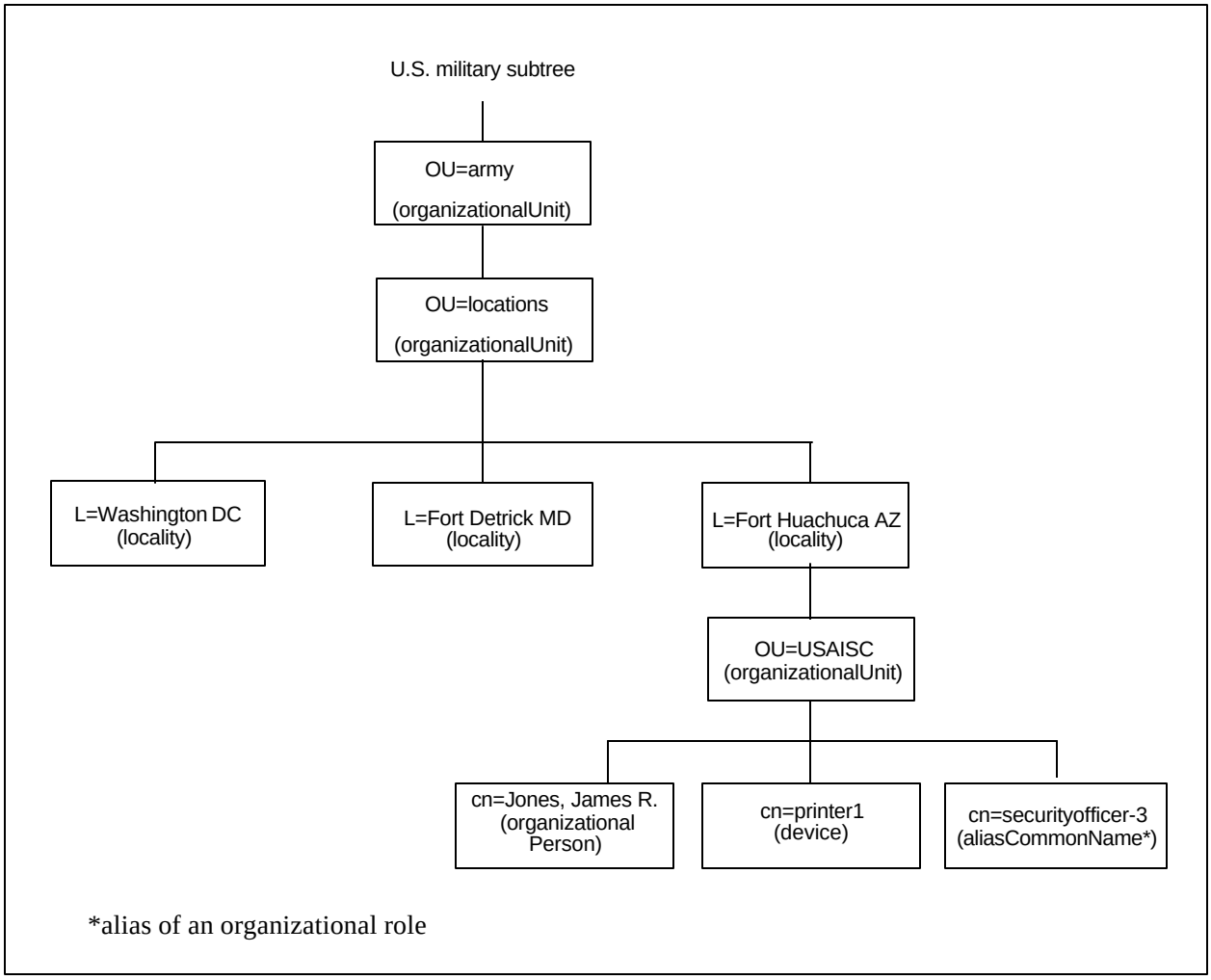

Figure B-11
Example Army Locations Directory Entries

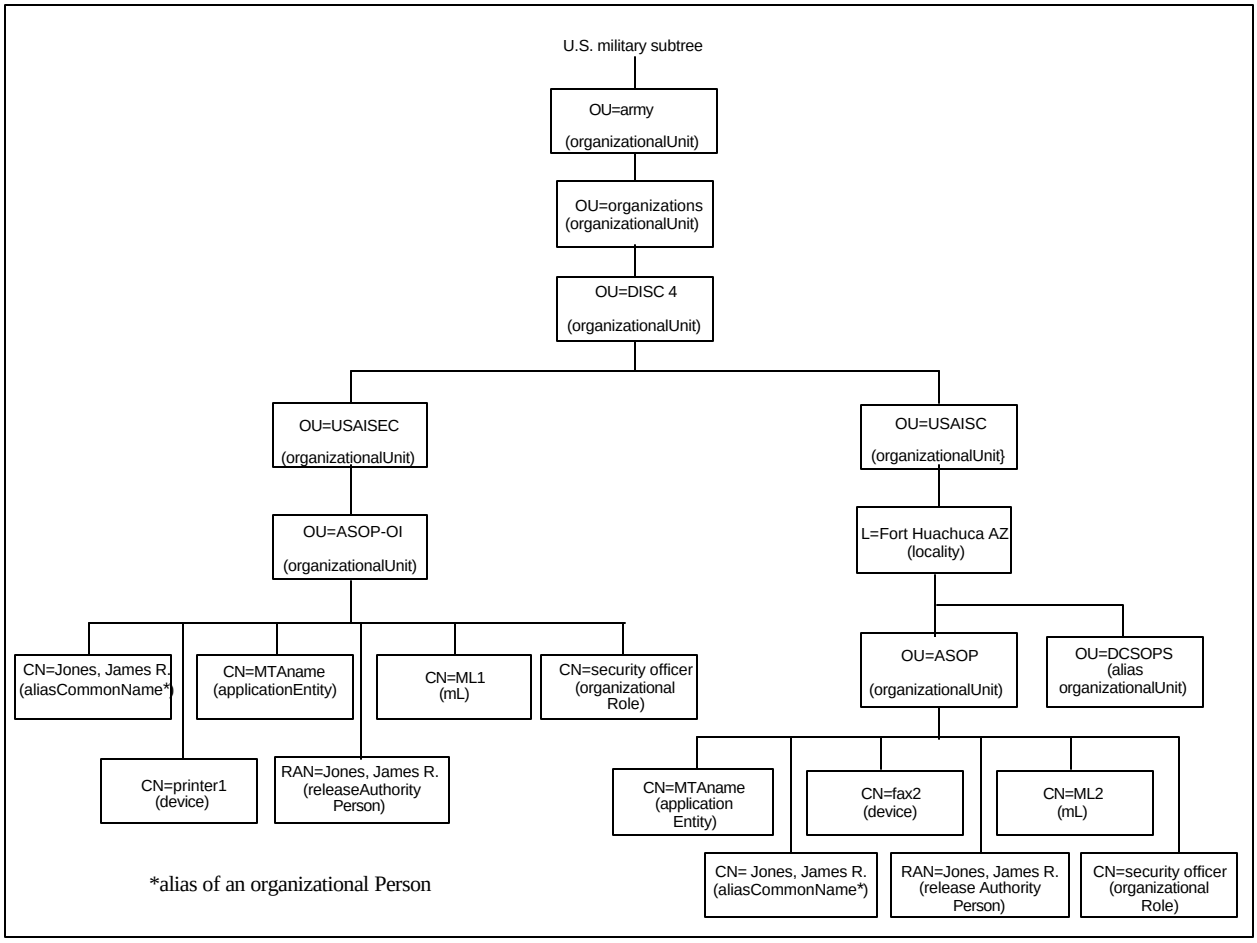

Figure B-12
Example Army Organizations Directory Entries

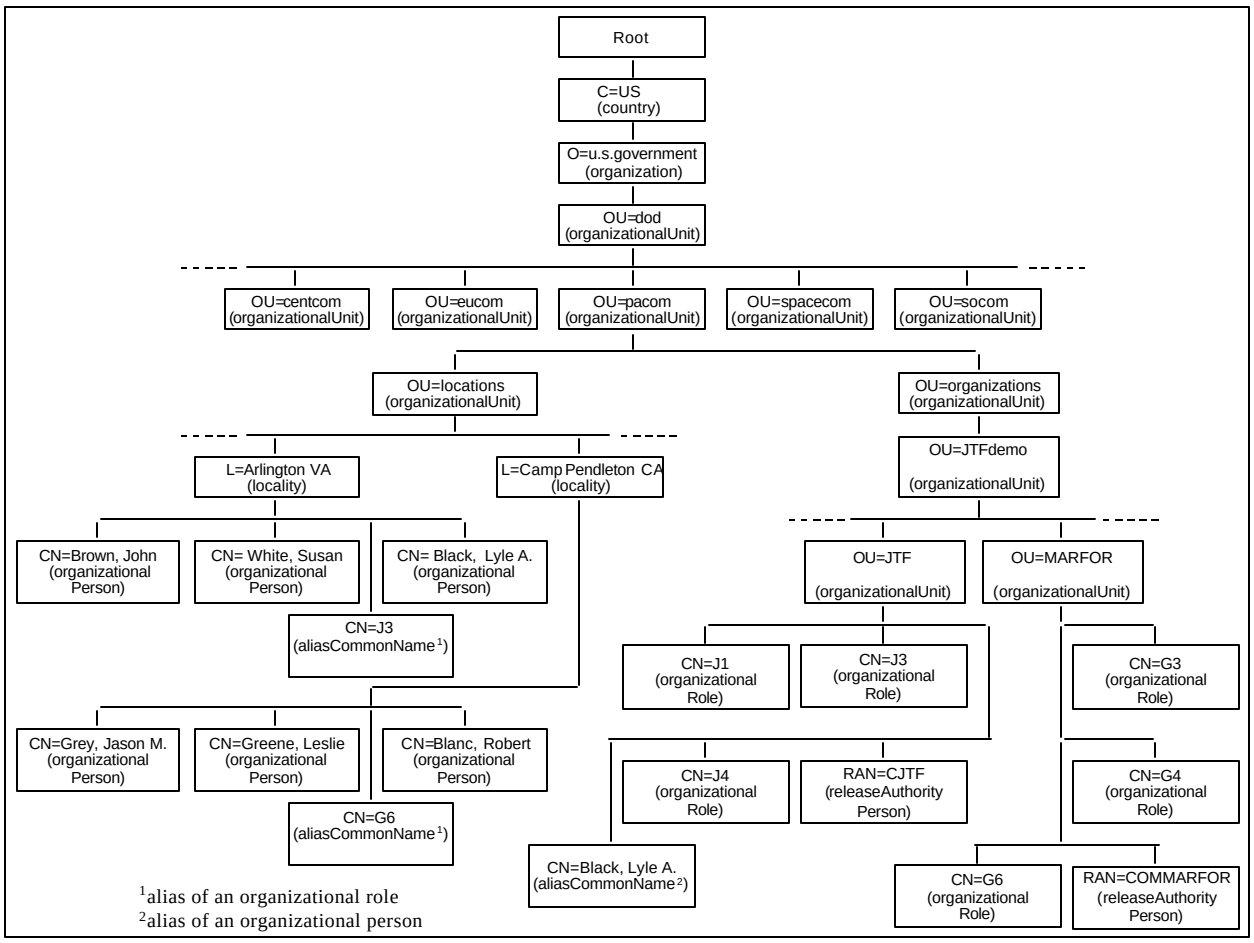

Figure B-13
Example PACOM Combined Task Force Directory Entries

SECTION XII

ACP 133 DATA TYPES

205. Example Content Rules

The following ASN.1 module specifies examples of content rules that realize the combinations given in Table B-54.

```
ACP133ExampleContentRules { joint-iso-ccitt(2) country(16) us(840) organization(1)
gov(101) dod(2) ds(2) module(0) contentRules(4) editionB(3) }

DEFINITIONS ::=
BEGIN

IMPORTS

CONTENT-RULE
    FROM InformationFramework {joint-iso-ccitt ds(5) module(1)
        informationFramework(1) 2 }

businessCategory, dnQualifier
    FROM SelectedAttributeTypes { joint-iso-ccitt ds(5) module(1)
        selectedAttributeTypes(5) 2 }

applicationEntity, cRLDistributionPoint, device, dSA, groupOfNames, locality,
organization, organizationalPerson, organizationalRole, organizationalUnit
    FROM SelectedObjectClasses { selectedObjectClasses 2 }
    -- Note that the object identifier value of the SelectedObjectClasses
    -- module is not changed by X.521 (1993) Amendment 1

supportedAlgorithms
    FROM CertificateExtensions { joint-iso-ccitt ds(5) module(1)
        certificateExtensions(26) 0 }

pkiCA
    FROM AuthenticationFramework {joint-iso-ccitt ds(5) module(1)
        authenticationFramework(7) 4 }

mhs-distribution-list, mhs-message-store, mhs-message-transfer-agent, mhs-user-agent,
mhs-user
    FROM MHSDirectoryObjectsAndAttributes { joint-iso-ccitt mhs motis(6) arch(5)
        modules(0) directory(1) version-1994(0) }

buildingName, rfc822Mailbox
    FROM { ccitt data(9) pss(2342) ucl(192003000) pilot(100) pilotAttributeType(1) 3 }

aCPLegacyFormat, addressList, aliasCommonName, aliasOrganizationalUnit,
aliasPointer, alternateRecipient, associatedAL, associatedOrganization, associatedPLA,
deployed, distributionCodeDescription, distributionCodesHandled, effectiveDate,
expirationDate, garrison, guard, listPointer, messagingGateway, mLAgent, nationality,
aCPNetworkEdB, aCPNetworkInstructionsEdB, otherContactInformation, plasServed,
plaUser, positionNumber, rank, releaseAuthorityPersonA, remarks, routingIndicator,
securePkiUser, serviceNumber, sigintPLA, spotPLA, tCCG, ukms
    FROM ACP133CommonContent { joint-iso-ccitt(2) country(16) us(840) organization(1)
        gov(101) dod(2) ds(2) module(0) commonContent(2) editionB (3) }

;  -- end of IMPORTS
```

```
        -- a. -- aCPApplicationEntityRuleEdA CONTENT-RULE
::= {
    STRUCTURAL OBJECT-CLASS     applicationEntity
    AUXILIARY OBJECT-CLASSES    { pkiCA |
                                  securePkiUser }
    MAY CONTAIN                 { aliasPointer |
                                  effectiveDate |
                                  dnQualifier |
                                  expirationDate
                                  }
}

        -- b. -- aCPCRLDistributionPointRule CONTENT-RULE
::= {
    STRUCTURAL OBJECT-CLASS     cRLDistributionPoint
    MAY CONTAIN                 { aliasPointer |
                                  effectiveDate |
                                  expirationDate }
}

        -- c. -- aCPDeviceRuleEdA CONTENT-RULE
::= {
    STRUCTURAL OBJECT-CLASS     device
    AUXILIARY OBJECT-CLASSES    { securePkiUser }
    MAY CONTAIN                 { aliasPointer |
                                  effectiveDate |
                                  expirationDate }
}

        -- d. -- aCPDSARuleEdA CONTENT-RULE
::= {
    STRUCTURAL OBJECT-CLASS     dSA
    AUXILIARY OBJECT-CLASSES    { securePkiUser }
    MAY CONTAIN                 { aliasPointer |
                                  effectiveDate |
                                  expirationDate }
}

        -- e. -- aCPGroupOfNamesRule CONTENT-RULE
::= {
    STRUCTURAL OBJECT-CLASS     groupOfNames
    MAY CONTAIN                 { aliasPointer |
                                  effectiveDate |
                                  expirationDate }
}
```

```
        -- f. -- aCPLocalityRule CONTENT-RULE
::= {
    STRUCTURAL OBJECT-CLASS     locality
    MAY CONTAIN                 { aliasPointer |
                                  effectiveDate |
                                  expirationDate }
}

        -- g. -- aCPMhs-distribution-listRule CONTENT-RULE
::= {
    STRUCTURAL OBJECT-CLASS     mhs-distribution-list
    MAY CONTAIN                 { aliasPointer |
                                  effectiveDate |
                                  expirationDate }
}

        -- h. -- aCPMhs-message-storeRuleEdA CONTENT-RULE
::= {
    STRUCTURAL OBJECT-CLASS     mhs-message-store
    AUXILIARY OBJECT-CLASSES    { securePkiUser }
    MAY CONTAIN                 { aliasPointer |
                                  effectiveDate |
                                  expirationDate }
}

        -- i. -- aCPMhs-message-transfer-agentRuleEdA CONTENT-RULE
::= {
    STRUCTURAL OBJECT-CLASS     mhs-message-transfer-agent
    AUXILIARY OBJECT-CLASSES    { securePkiUser }
    MAY CONTAIN                 { aliasPointer |
                                  effectiveDate |
                                  expirationDate }
}

        -- j. -- aCPMhs-user-agentRule CONTENT-RULE
::= {
    STRUCTURAL OBJECT-CLASS     mhs-user-agent
    MAY CONTAIN                 { aliasPointer |
                                  effectiveDate |
                                  expirationDate }
}
```

```
        -- k. -- aCPOrganizationalPersonRuleEdB CONTENT-RULE
::= {
    STRUCTURAL OBJECT-CLASS     organizationalPerson
    AUXILIARY OBJECT-CLASSES    { distributionCodesHandled |
                                  mhs-user |
                                  otherContactInformation |
                                  securePkiUser |
                                  ukms }
    MAY CONTAIN                 { aCPLegacyFormat |
                                  aliasPointer |
                                  alternateRecipient |
                                  businessCategory |
                                  deployed |
                                  dnQualifier |
                                  effectiveDate |
                                  expirationDate |
                                  garrison |
                                  guard |
                                  listPointer |
                                  nationality |
                                  positionNumber |
                                  rank |
                                  rfc822Mailbox |
                                  serviceNumber }
}

        -- l. -- aCPOrganizationalRoleRuleEdB CONTENT-RULE
::= {
    STRUCTURAL OBJECT-CLASS     organizationalRole
    AUXILIARY OBJECT-CLASSES    { pkiCA |
                                  distributionCodesHandled |
                                  mhs-user |
                                  otherContactInformation |
                                  securePkiUser |
                                  ukms }
    MAY CONTAIN                 { aCPLegacyFormat |
                                  aliasPointer |
                                  alternateRecipient |
                                  businessCategory |
                                  deployed |
                                  dnQualifier |
                                  effectiveDate |
                                  expirationDate |
                                  garrison |
                                  guard |
                                  listPointer |
                                  nationality |
                                  rfc822Mailbox }
}
```

```
        -- m. -- aCPOrganizationalUnitRuleEdB CONTENT-RULE
::= {
    STRUCTURAL OBJECT-CLASS     organizationalUnit
    AUXILIARY OBJECT-CLASSES    { pkiCA |
                                  distributionCodesHandled |
                                  mhs-user |
                                  otherContactInformation |
                                  plaUser |
                                  securePkiUser |
                                  ukms }
    MAY CONTAIN                 { aCPLegacyFormat |
                                  aliasPointer |
                                  alternateRecipient |
                                  associatedPLA |
                                  deployed |
                                  dnQualifier |
                                  effectiveDate |
                                  expirationDate |
                                  garrison |
                                  guard |
                                  listPointer |
                                  nationality |
                                  rfc822Mailbox }
}

        -- n. -- aCPOrganizationRuleEdB CONTENT-RULE
::= {
    STRUCTURAL OBJECT-CLASS     organization
    AUXILIARY OBJECT-CLASSES    { pkiCA |
                                  otherContactInformation }
    MAY CONTAIN                 { aCPLegacyFormat |
                                  aliasPointer |
                                  dnQualifier |
                                  effectiveDate |
                                  expirationDate }
}

        -- o. -- aCPRoutingIndicatorRuleEdB CONTENT-RULE
::= {
    STRUCTURAL OBJECT-CLASS     routingIndicator
    MAY CONTAIN                 { tCCG |
                                  remarks }
}
```

```
        -- p. -- addressListRuleEdA CONTENT-RULE
::= {
    STRUCTURAL OBJECT-CLASS     addressList
    AUXILIARY OBJECT-CLASSES    { distributionCodesHandled |
                                  mhs-user |
                                  plaUser |
                                  securePkiUser |
                                  ukms }
    MAY CONTAIN                 { aliasPointer |
                                  alternateRecipient |
                                  effectiveDate |
                                  expirationDate |
                                  guard |
                                  listPointer |
                                  rfc822Mailbox }
}

        -- q. -- aliasCommonNameRule CONTENT-RULE
::= {
    STRUCTURAL OBJECT-CLASS     aliasCommonName
    MAY CONTAIN                 { effectiveDate |
                                  expirationDate }
}

        -- r. -- aliasOrganizationalUnitRule CONTENT-RULE
::= {
    STRUCTURAL OBJECT-CLASS     aliasOrganizationalUnit
    MAY CONTAIN                 { effectiveDate |
                                  expirationDate }
}

        -- s. -- distributionCodeDescriptionRule CONTENT-RULE
::= {
    STRUCTURAL OBJECT-CLASS     distributionCodeDescription
    MAY CONTAIN                 { aliasPointer |
                                  effectiveDate |
                                  expirationDate }
}
```

```
        -- t. -- messagingGatewayRuleEdA CONTENT-RULE
::= {
    STRUCTURAL OBJECT-CLASS     messagingGateway
    AUXILIARY OBJECT-CLASSES    { securePkiUser |
                                  ukms}
    MAY CONTAIN                 { aliasPointer |
                                  effectiveDate |
                                  expirationDate |
                                  guard |
                                  plasServed |
                                  rfc822Mailbox }
}


        -- u. -- mLAgentRule CONTENT-RULE
::= {
    STRUCTURAL OBJECT-CLASS     mLAgent
    MAY CONTAIN                 { aliasPointer |
                                  effectiveDate |
                                  expirationDate }
}


        -- v. -- networkEdBRule CONTENT-RULE
::= {
    STRUCTURAL OBJECT-CLASS     aCPNetworkEdB
    MAY CONTAIN                 { effectiveDate |
                                  expirationDate }
}


        -- w. -- networkInstructionsEdBRule CONTENT-RULE
::= {
    STRUCTURAL OBJECT-CLASS     aCPNetworkInstructionsEdB
    MAY CONTAIN                 { effectiveDate |
                                  expirationDate }
}


        -- x. -- rAPersonRuleEdA CONTENT-RULE
::= {
    STRUCTURAL OBJECT-CLASS     releaseAuthorityPersonA
    MAY CONTAIN                 { effectiveDate  |
                                  expirationDate }
}
```

```
        -- y. -- sigintPLARule CONTENT-RULE
::= {
    STRUCTURAL OBJECT-CLASS     sigintPLA
    MAY CONTAIN                 { associatedOrganization }
}


        -- z. -- spotPLARule CONTENT-RULE
::= {
    STRUCTURAL OBJECT-CLASS     spotPLA
    MAY CONTAIN                 { associatedAL }
}

END  -- of ACP133ExampleContentRules module
```

206. Common Content ASN.1 Definitions

The following ASN.1 module specifies object classes, attributes, name forms, and other data types for the Allied Directory schema. This module imports only the data types used by the included definitions. That is, data types, that are part of the Common Content but are defined elsewhere and are not used in this module, e.g., the knowledgeInformation attribute, are not imported. Note that some definitions are included that are not used within this module, e.g., the aliasPointer attribute, but are used by the example content rules and are required in the Common Content.

207. Common Content Module

```
ACP133CommonContent { joint-iso-ccitt(2) country(16) us(840) organization(1) gov(101)
dod(2) ds(2) module(0) commonContent(2) editionB (3) }

DEFINITIONS ::=
BEGIN

IMPORTS

alias, ATTRIBUTE, auxiliary, DistinguishedName, distinguishedNameMatch, Name,
NAME-FORM, OBJECT-CLASS, objectIdentifierMatch, top
    FROM InformationFramework { joint-iso-ccitt ds(5) module(1)
            informationFramework(1) 2 }

selectedAttributeTypes, selectedObjectClasses, upperBounds
    FROM UsefulDefinitions { joint-iso-ccitt ds(5) module(1) usefulDefinitions(0) 2 }

attributeCertificate, SIGNED, userCertificate, pkiUser
    FROM AuthenticationFramework { joint-iso-ccitt ds(5) module(1)
            authenticationFramework(7) 4 }
```

supportedAlgorithms
FROM CertificateExtensions { joint-iso-ccitt ds(5) module(1) certificateExtensions(26) 0 }

bitStringMatch, booleanMatch, businessCategory, caseIgnoreListMatch, caseIgnoreListSubstringsMatch, caseIgnoreMatch, caseIgnoreSubstringsMatch, commonName, countryName, description, DirectoryString, distinguishedName, dnQualifier, generalizedTimeMatch, integerMatch, localityName, member, name, octetStringMatch, organizationalUnitName, organizationName, owner, seeAlso, stateOrProvinceName, telephoneNumber, telephoneNumberMatch, telephoneNumberSubstringsMatch,
FROM SelectedAttributeTypes { selectedAttributeTypes 2 }

applicationEntity, organizationalPerson, strongAuthenticationUser
FROM SelectedObjectClasses { selectedObjectClasses 2 }

ub-common-name
FROM UpperBounds upperBounds

mhs-distribution-list, mhs-dl-archive-service, mhs-dl-policy, mhs-dl-related-lists, mhs-dl-submit-permissions, mhs-dl-subscription-service, mhs-maximum-content-length, mhs-message-store, mhs-message-transfer-agent, mhs-or-addresses, mhs-user-agent
FROM MHSDirectoryObjectsAndAttributes { joint-iso-ccitt mhs motis(6) arch(5) modules(0) directory(1) version-1994(0) }

ORName
FROM MTSAbstractService { joint-iso-ccitt mhs-motis(6) mts(3) modules(0) mts-abstract-service(1) }

Kmid, MLReceiptPolicy, PairwiseTag
FROM CommonSecurityProtocol { joint-iso-ccitt 16 840 1 101 2 1 id-modules(0) id-csp(16) }

host, roomNumber
FROM { ccitt data(9) pss(2342) ucl(192003000) pilot(100) pilotAttributeType(1) 3 }

; -- end of IMPORTS

```
        -- a.  structural object classes


            -- (1) -- aCPNetworkEdB
::= {
    SUBCLASS OF       { top }
    MUST CONTAIN      { commonName }
    MAY CONTAIN       { description |
                        aCPNetworkSchemaEdB |
                        operationName |
                        seeAlso }
    ID                id-oc-aCPNetworkEdB
}


            -- (2) -- aCPNetworkInstructionsEdB OBJECT-CLASS
::= {
    SUBCLASS OF   { top }
    MUST CONTAIN  { commonName }
    MAY CONTAIN   { accessCodes |
                    aCPNetwAccessSchemaEdB |
                    description |
                    networkDN }
    ID            id-oc-aCPNetworkInstructionsEdB
}


            -- (3) -- addressList OBJECT-CLASS
::= {
    SUBCLASS OF   { top }
    MUST CONTAIN  { commonName |
                    mhs-dl-submit-permissions}
    MAY CONTAIN   { businessCategory |
                    copyMember |
                    description |
                    member |
                    mhs-dl-archive-service |
                    mhs-dl-policy |
                    mhs-dl-related-lists |
                    mhs-dl-subscription-service |
                    aLExemptedAddressProcessor |
                    alid |
                    aLReceiptPolicy |
                    aLType |
                    organizationalUnitName |
                    organizationName |
                    owner |
                    remarks |
                    seeAlso }
    ID                id-oc-addressList
}
```

```
        -- (4) -- aliasCommonName  OBJECT-CLASS
::= {
    SUBCLASS OF   { alias }
    MUST CONTAIN  { commonName }
    ID            id-oc-aliasCommonName
}

        -- (5) -- aliasOrganizationalUnit OBJECT-CLASS
::= {
    SUBCLASS OF       { alias }
    MUST CONTAIN      { organizationalUnitName }
    ID                id-oc-aliasOrganizationalUnit
}

        -- (6) -- altSpellingACP127 OBJECT-CLASS
::= {
    SUBCLASS OF   { plaACP127 }
    MUST CONTAIN { plaReplace |
                   primarySpellingACP127 }
    ID            id-oc-altSpellingACP127
}

        -- (7) -- cadACP127.OBJECT-CLASS.
::= {
    SUBCLASS OF   { plaACP127 }
    MUST CONTAIN  { cognizantAuthority}
    MAY CONTAIN   { associatedAL |
                   entryClassification |
                   recapDueDate |
                   rlInfo }
    ID            id-oc-cadACP127
}

        -- (8) -- distributionCodeDescription OBJECT-CLASS
::= {
    SUBCLASS OF   { top }
    MUST CONTAIN  { commonName }
    MAY CONTAIN   { description }
    ID            id-oc-distributionCodeDescription
}
```

```
        -- (9) -- dSSCSPLA OBJECT-CLASS
    ::= {
        SUBCLASS OF     { plaACP127 }
        MUST CONTAIN    { rl }
        MAY CONTAIN     { adminConversion |
                          associatedOrganization |
                          localityName |
                          sigad |
                          usdConversion }
        ID              id-oc-dSSCSPLA
    }


        -- (10) -- messagingGateway OBJECT-CLASS
::= {
    SUBCLASS OF   { mhs-message-transfer-agent }
    MAY CONTAIN   { administrator |
                    aigsExpanded |
                    gatewayType |
                    ghpType |
                    host |
                    mailDomains |
                    mhs-acceptable-eits |
                    mhs-deliverable-content-types |
                    mhs-exclusively-acceptable-eits |
                    mhs-message-store-dn |
                    mhs-or-addresses |
                    mhs-or-addresses-with-capabilities |
                    mhs-unacceptable-eits |
                    onSupported |
                    plaNameACP127 |
                    rlInfo }
    ID            id-oc-messagingGateway
}


        -- (11) -- mLA OBJECT-CLASS
::= {
    SUBCLASS OF   { applicationEntity |
                    strongAuthenticationUser }
    MAY CONTAIN   { supportedAlgorithms}
    ID            id-oc-mLA
}
```

```
        -- (12) -- mLAgent OBJECT-CLASS
::= {
    SUBCLASS OF   { applicationEntity |
                    pkiUser }
    MAY CONTAIN   { supportedAlgorithms}
    ID            id-oc-mLAgent
}


        -- (13) -- network OBJECT-CLASS
::= {
    SUBCLASS OF       { top }
    MUST CONTAIN      { commonName }
    MAY CONTAIN       { description |
                        networkSchema |
                        operationName |
                        seeAlso }
    ID                id-oc-network
}


        -- (14) -- networkInstructions OBJECT-CLASS
::= {
    SUBCLASS OF   { top }
    MUST CONTAIN  { commonName }
    MAY CONTAIN   { accessCodes |
                    accessSchema |
                    description |
                    networkDN }
    ID            id-oc-networkInstructions
}
```

```
        -- (15) -- orgACP127 OBJECT-CLASS
::= {
    SUBCLASS OF   { plaACP127 }
    MAY CONTAIN   { accountingCode |
                    associatedOrganization |
                    countryName |
                    dualRoute |
                    entryClassification |
                    localityName |
                    longTitle |
                    minimize |
                    minimizeOverride |
                    nameClassification |
                    rl |
                    rlInfo |
                    section |
                    stateOrProvinceName |
                    tARE }
    ID            id-oc-orgACP127
}

        -- (16) -- plaCollectiveACP127 OBJECT-CLASS
::= {
    SUBCLASS OF   { plaACP127 }
    MUST CONTAIN  { cognizantAuthority }
    MAY CONTAIN   { actionAddressees |
                    allowableOriginators |
                    associatedAL |
                    description |
                    entryClassification |
                    infoAddressees |
                    lastRecapDate |
                    recapDueDate }
    ID            id-oc-plaCollectiveACP127
}

        -- (17) -- releaseAuthorityPerson OBJECT-CLASS
::= {
    SUBCLASS OF   { secure-user }
    MUST CONTAIN  { releaseAuthorityName }
    ID            id-oc-releaseAuthorityPerson
}
```

```
        -- (18) -- releaseAuthorityPersonA OBJECT-CLASS
::= {
    SUBCLASS OF   { securePkiUser }
    MUST CONTAIN  { releaseAuthorityName }
    ID            id-oc-releaseAuthorityPersonA
}


        -- (19) -- routingIndicator OBJECT-CLASS
::= {
    SUBCLASS OF   { plaData }
    MUST CONTAIN  { rI }
    MAY CONTAIN   { lmf |
                    mhs-maximum-content-length |
                    nationality |
                    publish |
                    rIClassification |
                    sHD |
                    tCC |
                    transferStation |
                    tRC }
    ID            id-oc-routingIndicator
}


        -- (20) -- sigintPLA OBJECT-CLASS
::= {
    SUBCLASS OF   { plaData }
    MUST CONTAIN  { sigad }
    MAY CONTAIN   { localityName |
                    nationality |
                    publish |
                    remarks |
                    rI |
                    shortTitle }
    ID            id-oc-sigintPLA
}
```

```
        -- (21) -- slPLA OBJECT-CLASS
::= {
    SUBCLASS OF   { plaData }
    MUST CONTAIN  { longTitle }
    MAY CONTAIN   { localityName |
                    nationality |
                    publish |
                    remarks |
                    rl |
                    shortTitle |
                    sigad }
    ID            id-oc-slPLA
}

        -- (22) -- spotPLA OBJECT-CLASS
::= {
    SUBCLASS OF   { plaData }
    MUST CONTAIN  { spot }
    MAY CONTAIN   { actionAddressees |
                    additionalAddressees |
                    additionalSecondPartyAddressees |
                    mhs-dl-submit-permissions |
                    remarks |
                    secondPartyAddressees }
    ID            id-oc-spotPLA
}

        -- (23) -- taskForceACP127 OBJECT-CLASS
::= {
    SUBCLASS OF   { plaACP127 }
    MUST CONTAIN  { cognizantAuthority |
                    lastRecapDate |
                    recapDueDate}
    MAY CONTAIN   { associatedAL |
                    entryClassification |
                    plaAddressees }
    ID            id-oc-taskForceACP127
}

        -- (24) -- tenantACP127 OBJECT-CLASS
::= {
    SUBCLASS OF   { plaACP127 }
    MUST CONTAIN  { hostOrgACP127 }
    MAY CONTAIN   { entryClassification |
                    tARE }
    ID            id-oc-tenantACP127
}
```

```
        -- b.  auxiliary object classes


            -- (1) -- distributionCodesHandled OBJECT-CLASS
::= {
    SUBCLASS OF   {top}
    KIND          auxiliary
    MAY CONTAIN   { distributionCodeAction |
                    distributionCodeInfo }
    ID            id-oc-distributionCodesHandled
}


            -- (2) -- otherContactInformation OBJECT-CLASS
::= {
    SUBCLASS OF   { top }
    KIND          auxiliary
    MAY CONTAIN   { aCPMobileTelephoneNumber |
                    aCPPagerTelephoneNumber |
                    aCPPreferredDelivery |
                    mailDomains |
                    militaryFacsimileNumber |
                    militaryTelephoneNumber |
                    proprietaryMailboxes |
                    roomNumber |
                    secureFacsimileNumber |
                    secureTelephoneNumber }
    ID            id-oc-otherContactInformation
}


            -- (3) -- plaACP127 OBJECT-CLASS
::= {
    SUBCLASS OF   { top }
    KIND          auxiliary
    MUST CONTAIN  { plaNameACP127 }
    MAY CONTAIN   { community |
                    effectiveDate |
                    expirationDate |
                    nationality |
                    publish |
                    remarks |
                    serviceOrAgency }
    ID            id-oc-plaACP127
}
```

```
        -- (4) -- plaData OBJECT-CLASS
::= {
    SUBCLASS OF   { top }
    KIND          auxiliary
    MAY CONTAIN   { community |
                    description |
                    effectiveDate |
                    expirationDate }
    ID            id-oc-plaData
}

        -- (5) -- plaUser OBJECT-CLASS
::= {
    SUBCLASS OF   { top }
    KIND          auxiliary
    MUST CONTAIN  { plaNameACP127 }
    MAY CONTAIN   { rIInfo }
    ID            id-oc-plaUser
}

        -- (6) -- secure-user OBJECT-CLASS
::= {
    SUBCLASS OF   { strongAuthenticationUser }
    KIND          auxiliary
    MAY CONTAIN   { attributeCertificate |
                    supportedAlgorithms }
    ID            id-oc-secure-user
}

        -- (7) -- securePkiUser OBJECT-CLASS
::= {
    SUBCLASS OF   { pkiUser }
    KIND          auxiliary
    MAY CONTAIN   { attributeCertificate |
                    supportedAlgorithms }
    ID            id-oc-securePkiUser
}
```

```
        -- (8) -- ukms OBJECT-CLASS
::= {
    SUBCLASS OF   { top }
    KIND          auxiliary
    MAY CONTAIN   { janUKMs |
                    febUKMs |
                    marUKMs |
                    aprUKMs |
                    mayUKMs |
                    junUKMs |
                    julUKMs |
                    augUKMs |
                    sepUKMs |
                    octUKMs |
                    novUKMs |
                    decUKMs }
    ID            id-oc-ukms
}


    -- c.  attribute types


        -- (1) -- accessCodes ATTRIBUTE
::= {
    WITH SYNTAX    PrintableString
    ID          id-at-accessCodes
}


        -- (2) -- accessSchema ATTRIBUTE
::= {
    WITH SYNTAX    GraphicString
    ID             id-at-accessSchema
}


        -- (3) -- accountingCode ATTRIBUTE
::= {
    WITH SYNTAX                   PrintableString (SIZE (1..7))
    EQUALITY MATCHING RULE        caseIgnoreMatch
    SUBSTRINGS MATCHING RULE      caseIgnoreSubstringsMatch
    ID                            id-at-accountingCode
}
```

```
        -- (4) -- aCPLegacyFormat ATTRIBUTE
::={
    WITH SYNTAX     ACPLegacyFormat
    SINGLE VALUE    TRUE
    ID              id-at-aCPLegacyFormat
}


        -- (5) -- aCPMobileTelephoneNumber ATTRIBUTE
::= {
    SUBTYPE OF      telephoneNumber
    ID              id-at-aCPMobileTelephoneNumber
}


        -- (6) -- aCPNetwAccessSchemaEdB ATTRIBUTE
::= {
    WITH SYNTAX     JPEG  -- values of the string are JPEG- formatted
                          -- (JFIF) photographs
    ID              id-at-aCPNetwAccessSchemaEdB
}


        -- (7) -- aCPNetworkSchemaEdB ATTRIBUTE
::= {
    WITH SYNTAX     JPEG  -- values of the string are JPEG- formatted
                    -- (JFIF) photographs
    ID              id-at-aCPNetworkSchemaEdB
}


        -- (8) -- aCPPagerTelephoneNumber ATTRIBUTE
::= {
    SUBTYPE OF      telephoneNumber
    ID              id-at-aCPPagerTelephoneNumber
}


        -- (9) -- aCPPreferredDelivery ATTRIBUTE
::= {
    WITH SYNTAX     ENUMERATED { SMTP(0), ACP127(1), MHS(2) }
    SINGLE VALUE    TRUE
    ID              id-at-aCPPreferredDelivery
}
```

```
        -- (10) -- aCPTelephoneFaxNumber ATTRIBUTE
::= {
    WITH SYNTAX                     ACPTelephoneFaxNumberSyntax
    EQUALITY MATCHING RULE          telephoneNumberMatch
    SUBSTRINGS MATCHING RULE        telephoneNumberSubstringsMatch
    ID                              id-at-aCPTelephoneFaxNumber
}

        -- (11) -- actionAddressees ATTRIBUTE
::= {
    WITH SYNTAX                     Addressees
    EQUALITY MATCHING RULE          caseIgnoreListMatch
    SUBSTRINGS MATCHING RULE        caseIgnoreListSubstringsMatch
    ID                              id-at-actionAddressees
}

        -- (12) -- additionalAddressees ATTRIBUTE
::= {
    WITH SYNTAX                     Addressees
    EQUALITY MATCHING RULE          caseIgnoreListMatch
    SUBSTRINGS MATCHING RULE        caseIgnoreListSubstringsMatch
    ID                              id-at-additionalAddressees
}

        -- (13) -- additionalSecondPartyAddressees ATTRIBUTE
::={
    WITH SYNTAX                     Addressees
    EQUALITY MATCHING RULE          caseIgnoreListMatch
    SUBSTRINGS MATCHING RULE        caseIgnoreListSubstringsMatch
    ID                              id-at-additionalSecondPartyAddressees
}

        -- (14) -- adminConversion ATTRIBUTE
::={
    WITH SYNTAX                     DirectoryString
    EQUALITY MATCHING RULE          caseIgnoreMatch
    SUBSTRING MATCHING RULE         caseIgnoreSubstringsMatch
    ID                              id-at-adminConversion
}

        -- (15) -- administrator ATTRIBUTE
::= {
    SUBTYPE OF      distinguishedName
    ID              id-at-administrator
}
```

```
        -- (16) -- aigsExpanded ATTRIBUTE
::= {
    SUBTYPE OF      distinguishedName
    ID              id-at-aigsExpanded
}

        -- (17) -- aLExemptedAddressProcessor ATTRIBUTE
::= {
    WITH SYNTAX     ORName
    SINGLE VALUE    TRUE
    ID              id-at-aLExemptedAddressProcessor
}

        -- (18) -- aliasPointer ATTRIBUTE
::= {
    WITH SYNTAX                 DistinguishedName
    EQUALITY MATCHING RULE      distinguishedNameMatch
    ID                          id-at-aliasPointer
}

        -- (19) -- alid ATTRIBUTE
::= {
    WITH SYNTAX                 Kmid
    EQUALITY MATCHING RULE      octetStringMatch
    ID                          id-at-alid
}

        -- (20) -- allowableOriginators ATTRIBUTE
::= {
    WITH SYNTAX                 Addressees
    EQUALITY MATCHING RULE      caseIgnoreListMatch
    SUBSTRINGS MATCHING RULE    caseIgnoreListSubstringsMatch
    ID                          id-at-allowableOriginators
}

        -- (21) -- aLReceiptPolicy ATTRIBUTE
::= {
    WITH SYNTAX     MLReceiptPolicy
    SINGLE VALUE    TRUE
    ID              id-at-aLReceiptPolicy
}
```

```
        -- (22) -- alternateRecipient ATTRIBUTE
::= {
    WITH SYNTAX                 DistinguishedName
    EQUALITY MATCHING RULE      distinguishedNameMatch
    ID                          id-at-alternateRecipient
}

        -- (23) -- aLType ATTRIBUTE
::= {
    WITH SYNTAX                 INTEGER { AIG(0), TYPE(1), CAD(2), TASKFORCE(3),
                                          DAG(4) }
    EQUALITY MATCHING RULE      integerMatch
    SINGLE VALUE                TRUE
    ID                          id-at-aLType
}

        -- (24) -- aprUKMs ATTRIBUTE
::= {
    WITH SYNTAX     MonthlyUKMs
    SINGLE VALUE    TRUE
    ID              id-at-aprUKMs
}

        -- (25) -- associatedAL ATTRIBUTE
::= {
    WITH SYNTAX                 DistinguishedName
    EQUALITY MATCHING RULE      distinguishedNameMatch
    ID                          id-at-associatedAL
}

        -- (26) -- associatedOrganization ATTRIBUTE
::= {
    WITH SYNTAX                 DistinguishedName
    EQUALITY MATCHING RULE      distinguishedNameMatch
    ID                          id-at-associatedOrganization
}

        -- (27) -- associatedPLA ATTRIBUTE
::= {
    WITH SYNTAX                 DistinguishedName
    EQUALITY MATCHING RULE      distinguishedNameMatch
    ID                          id-at-associatedPLA
}
```

```
        -- (28) -- augUKMs ATTRIBUTE
::= {
    WITH SYNTAX     MonthlyUKMs
    SINGLE VALUE    TRUE
    ID              id-at-augUKMs
}

        -- (29) -- cognizantAuthority ATTRIBUTE
::= {
    WITH SYNTAX                     PrintableString (SIZE (1..55))
    EQUALITY MATCHING RULE          caseIgnoreMatch
    SUBSTRINGS MATCHING RULE        caseIgnoreSubstringsMatch
    SINGLE VALUE                    TRUE
    ID                              id-at-cognizantAuthority
}

        -- (30) -- community ATTRIBUTE
::= {
    WITH SYNTAX     ENUMERATED { GENSER(0), SI(1), Both(2) }
    SINGLE VALUE    TRUE
    ID              id-at-community
}

        -- (31) -- copyMember ATTRIBUTE
::= {
    SUBTYPE OF      member
    ID              id-at-copyMember
}

        -- (32) -- decUKMs ATTRIBUTE
::= {
    WITH SYNTAX     MonthlyUKMs
    SINGLE VALUE    TRUE
    ID              id-at-decUKMs
}

        -- (33) -- deployed ATTRIBUTE
::= {
    WITH SYNTAX                 DistinguishedName
    EQUALITY MATCHING RULE      distinguishedNameMatch
    ID                          id-at-deployed
}
```

```
        -- (34) -- distributionCodeAction ATTRIBUTE
::= {
    WITH SYNTAX                     DistributionCode
    EQUALITY MATCHING RULE          caseIgnoreMatch
    SUBSTRINGS MATCHING RULE        caseIgnoreSubstringsMatch
    ID                              id-at-distributionCodeAction
}

        -- (35) -- distributionCodeInfo ATTRIBUTE
::= {
    WITH SYNTAX                     DistributionCode
    EQUALITY MATCHING RULE          caseIgnoreMatch
    SUBSTRINGS MATCHING RULE        caseIgnoreSubstringsMatch
    ID                              id-at-distributionCodeInfo
}

        -- (36) -- dualRoute ATTRIBUTE
::= {
    WITH SYNTAX                     BOOLEAN
    EQUALITY MATCHING RULE          booleanMatch
    SINGLE VALUE                    TRUE
    ID                              id-at-dualRoute
}

        -- (37) -- effectiveDate ATTRIBUTE
::= {
    WITH SYNTAX                     GeneralizedTime
    EQUALITY MATCHING RULE          generalizedTimeMatch
    SINGLE VALUE                    TRUE
    ID                              id-at-effectiveDate
}

        -- (38) -- entryClassification ATTRIBUTE
::= {
    WITH SYNTAX     Classification
    ID              id-at-entryClassification
}

        -- (39) -- expirationDate ATTRIBUTE
::= {
    WITH SYNTAX                     GeneralizedTime
    EQUALITY MATCHING RULE          generalizedTimeMatch
    SINGLE VALUE                    TRUE
    ID                              id-at-expirationDate
}
```

```
        -- (40) -- febUKMs ATTRIBUTE
::= {
    WITH SYNTAX     MonthlyUKMs
    SINGLE VALUE    TRUE
    ID              id-at-febUKMs
}


        -- (41) -- garrison ATTRIBUTE
::= {
    WITH SYNTAX                 DistinguishedName
    EQUALITY MATCHINGRULE       distinguishedNameMatch
    ID                          id-at-garrison
}


        -- (42) -- gatewayType ATTRIBUTE
::= {
    WITH SYNTAX                 OBJECT IDENTIFIER
    EQUALITY MATCHING RULE      objectIdentifierMatch
    ID                          id-at-gatewayType
}


        -- (43) -- ghpType ATTRIBUTE
::= {
    WITH SYNTAX                 OBJECT IDENTIFIER
    EQUALITY MATCHING RULE      objectIdentifierMatch
    ID                          id-at-ghpType
}


        -- (44) -- guard ATTRIBUTE
::= {
    SUBTYPE OF      distinguishedName
    ID              id-at-guard
}


        -- (45) -- hostOrgACP127 ATTRIBUTE
::= {
    WITH SYNTAX                 PrintableString (SIZE (1..55))
    EQUALITY MATCHING RULE      caseIgnoreMatch
    SUBSTRINGS MATCHING RULE    caseIgnoreSubstringsMatch
    SINGLE VALUE                TRUE
    ID                          id-at-hostOrgACP127
}
```

```
        -- (46) -- infoAddressees ATTRIBUTE
::= {
    WITH SYNTAX                     Addressees
    EQUALITY MATCHING RULE          caseIgnoreListMatch
    SUBSTRINGS MATCHING RULE        caseIgnoreListSubstringsMatch
    ID                              id-at-infoAddressees
}


        -- (47) -- janUKMs ATTRIBUTE
::= {
    WITH SYNTAX     MonthlyUKMs
    SINGLE VALUE    TRUE
    ID              id-at-janUKMs
}


        -- (48) -- julUKMs ATTRIBUTE
::= {
    WITH SYNTAX     MonthlyUKMs
    SINGLE VALUE    TRUE
    ID              id-at-julUKMs
}


        -- (49) -- junUKMs ATTRIBUTE
::= {
    WITH SYNTAX     MonthlyUKMs
    SINGLE VALUE    TRUE
    ID              id-at-junUKMs
}


        -- (50) -- lastRecapDate ATTRIBUTE
::= {
    WITH SYNTAX                     GeneralizedTime
    EQUALITY MATCHING RULE          generalizedTimeMatch
    SINGLE VALUE                    TRUE
    ID                              id-at-lastRecapDate
}


        -- (51) -- listPointer ATTRIBUTE
::= {
    WITH SYNTAX                     DistinguishedName
    EQUALITY MATCHING RULE          distinguishedNameMatch
    ID                              id-at-listPointer
}
```

```
        -- (52) -- lmf ATTRIBUTE
::= {
    WITH SYNTAX                 PrintableString (SIZE (1))
    EQUALITY MATCHING RULE      caseIgnoreMatch
    SINGLE VALUE                TRUE
    ID                          id-at-lmf
}

        -- (53) -- longTitle ATTRIBUTE
::= {
    WITH SYNTAX                 PrintableString (SIZE (1...255))
    EQUALITY MATCHING RULE      caseIgnoreMatch
    SUBSTRINGS MATCHING RULE    caseIgnoreSubstringsMatch
    SINGLE VALUE                TRUE
    ID                          id-at-longTitle
}

        -- (54) -- mailDomains ATTRIBUTE
::= {
    WITH SYNTAX                 DirectoryString
    EQUALITY MATCHING RULE      caseIgnoreMatch
    SUBSTRINGS MATCHING RULE    caseIgnoreSubstringsMatch
    ID                          id-at-mailDomains
}

        -- (55) -- marUKMs ATTRIBUTE
::= {
    WITH SYNTAX     MonthlyUKMs
    SINGLE VALUE    TRUE
    ID              id-at-marUKMs
}

        -- (56) -- mayUKMs ATTRIBUTE
::= {
    WITH SYNTAX     MonthlyUKMs
    SINGLE VALUE    TRUE
    ID              id-at-mayUKMs
}

        -- (57) -- militaryFacsimileNumber ATTRIBUTE
::= {
    SUBTYPE OF      aCPTelephoneFaxNumber
    ID              id-at-militaryFacsimileNumber
}
```

```
        -- (58) -- militaryTelephoneNumber ATTRIBUTE
::= {
    SUBTYPE OF      aCPTelephoneFaxNumber
    ID              id-at-militaryTelephoneNumber
}

        -- (59) -- minimize ATTRIBUTE
::= {
    WITH SYNTAX             BOOLEAN
EQUALITY MATCHING RULE      booleanMatch
SINGLE VALUE                TRUE
ID                          id-at-minimize
}

        -- (60) -- minimizeOverride ATTRIBUTE
::= {
    WITH SYNTAX             BOOLEAN
EQUALITY MATCHING RULE      booleanMatch
SINGLE VALUE                TRUE
ID                          id-at-minimizeOverride
}

        -- (61) -- nameClassification ATTRIBUTE
::= {
    WITH SYNTAX     Classification
    ID              id-at-nameClassification
}

        -- (62) -- nationality ATTRIBUTE
::= {
    SUBTYPE OF      name
    WITH SYNTAX     PrintableString (SIZE (2))  -- ISO 3166 codes only
    SINGLE VALUE    TRUE
    ID              id-at-nationality
}

        -- (63) -- networkDN ATTRIBUTE
::= {
    WITH SYNTAX             DistinguishedName
    EQUALITY MATCHING RULE  distinguishedNameMatch
    ID                      id-at-networkDN
}
```

```
        -- (64) -- networkSchema ATTRIBUTE
::= {
    WITH SYNTAX     GraphicString
    ID              id-at-networkSchema
}


        -- (65) -- novUKMs ATTRIBUTE
::= {
    WITH SYNTAX     MonthlyUKMs
    SINGLE VALUE    TRUE
    ID              id-at-novUKMs
}


        -- (66) -- octUKMs ATTRIBUTE
::= {
    WITH SYNTAX     MonthlyUKMs
    SINGLE VALUE    TRUE
    ID              id-at-octUKMs
}


        -- (67) -- onSupported ATTRIBUTE
::= {
    WITH SYNTAX         BIT STRING { acp127-nn(0), acp127-pn(1), acp127-tn(2) }
    EQUALITY MATCHING RULE   bitStringMatch
    SINGLE VALUE            TRUE
    ID              id-at-onSupported
}


        -- (68) -- operationName ATTRIBUTE
::= {
    WITH SYNTAX                     DirectoryString
    EQUALITY MATCHING RULE          caseIgnoreMatch
    SUBSTRINGS MATCHING RULE        caseIgnoreSubstringsMatch
    ID                              id-at-operationName
}


        -- (69) -- plaAddressees ATTRIBUTE
::= {
    WITH SYNTAX                     Addressees
    EQUALITY MATCHING RULE          caseIgnoreListMatch
    SUBSTRINGS MATCHING RULE        caseIgnoreListSubstringsMatch
    ID                              id-at-plaAddressees
}
```

```
        -- (70) -- plaNameACP127 ATTRIBUTE
::= {
    SUBTYPE OF name
    WITH SYNTAX     PrintableString (SIZE (1..55))
    SINGLE VALUE    TRUE
    ID              id-at-plaNameACP127
}


        -- (71) -- plaReplace ATTRIBUTE
::= {
    WITH SYNTAX                 BOOLEAN
    EQUALITY MATCHING RULE      booleanMatch
    SINGLE VALUE                TRUE
    ID                          id-at-plaReplace
}


        -- (72) -- plasServed ATTRIBUTE
::= {
    SUBTYPE OF name
ID              id-at-plasServed
}


        -- (73) -- positionNumber ATTRIBUTE
::= {
    WITH SYNTAX                 DirectoryString
    EQUALITY MATCHING RULE      caseIgnoreMatch
    SUBSTRINGS MATCHING RULE    caseIgnoreSubstringsMatch
    ID                          id-at-positionNumber
}


        -- (74) -- primarySpellingACP127 ATTRIBUTE
::= {
    WITH SYNTAX                 PrintableString (SIZE (1..55))
    EQUALITY MATCHING RULE      caseIgnoreMatch
    SUBSTRINGS MATCHING RULE    caseIgnoreSubstringsMatch
    SINGLE VALUE                TRUE
    ID                          id-at-primarySpellingACP127
}


        -- (75) -- proprietaryMailboxes ATTRIBUTE
::= {
    WITH SYNTAX                 DirectoryString
    EQUALITY MATCHING RULE      caseIgnoreMatch
    SUBSTRINGS MATCHING RULE    caseIgnoreSubstringsMatch
    ID                          id-at-proprietaryMailboxes
}
```

```
        -- (76) -- publish ATTRIBUTE
::= {
    WITH SYNTAX                 BOOLEAN
    EQUALITY MATCHING RULE      booleanMatch
    SINGLE VALUE                TRUE
    ID                          id-at-publish
}

        -- (77) -- rank ATTRIBUTE
::= {
    WITH SYNTAX                 DirectoryString
    EQUALITY MATCHING RULE      caseIgnoreMatch
    SUBSTRINGS MATCHING RULE    caseIgnoreSubstringsMatch
    ID                          id-at-rank
}

        -- (78) -- recapDueDate ATTRIBUTE
::= {
    WITH SYNTAX                 GeneralizedTime
    EQUALITY MATCHING RULE      generalizedTimeMatch
    SINGLE VALUE                TRUE
    ID                          id-at-recapDueDate
}

        -- (79) -- releaseAuthorityName ATTRIBUTE
::= {
    WITH SYNTAX                 DirectoryString (SIZE (1..ub-common-name))
    EQUALITY MATCHING RULE      caseIgnoreMatch
    SUBSTRINGS MATCHING RULE    caseIgnoreSubstringsMatch
    ID                          id-at-releaseAuthorityName
}

        -- (80) -- remarks ATTRIBUTE
::= {
    WITH SYNTAX                 Remarks
    EQUALITY MATCHING RULE      caseIgnoreListMatch
    ID                          id-at-remarks
}
```

```
        -- (81) -- rl ATTRIBUTE
::= {
    WITH SYNTAX                     PrintableString
    EQUALITY MATCHING RULE          caseIgnoreMatch
    SUBSTRINGS MATCHING RULE        caseIgnoreSubstringsMatch
    ID                              id-at-rl
}

        -- (82) -- rlClassification ATTRIBUTE
::= {
    WITH SYNTAX     Classification
    ID              id-at-rlClassification
}

        -- (83) -- rlInfo ATTRIBUTE
::= {
    WITH SYNTAX     RIParameters
    ID              id-at-rlInfo
}

        -- (84) -- secondPartyAddressees ATTRIBUTE
::= {
    WITH SYNTAX                     Addressees
    EQUALITY MATCHING RULE          caseIgnoreListMatch
    SUBSTRINGS MATCHING RULE        caseIgnoreListSubstringsMatch
    ID                              id-at-secondPartyAddressees
}

        -- (85) -- section ATTRIBUTE
::= {
    WITH SYNTAX                     BOOLEAN
    EQUALITY MATCHING RULE          booleanMatch
    SINGLE VALUE                    TRUE
    ID                              id-at-section
}

        -- (86) -- secureFacsimileNumber ATTRIBUTE
::= {
    SUBTYPE OF      aCPTelephoneFaxNumber
    ID              id-at-secureFacsimileNumber
}
```

```
        -- (87) -- secureTelephoneNumber ATTRIBUTE
::= {
    SUBTYPE OF      aCPTelephoneFaxNumber
    ID              id-at-secureTelephoneNumber
}

        -- (88) -- sepUKMs ATTRIBUTE
::= {
    WITH SYNTAX     MonthlyUKMs
    SINGLE VALUE    TRUE
    ID              id-at-sepUKMs
}

        -- (89) -- serviceNumber ATTRIBUTE
::= {
    WITH SYNTAX                     DirectoryString
    EQUALITY MATCHING RULE          caseIgnoreMatch
    SUBSTRINGS MATCHING RULE        caseIgnoreSubstringsMatch
    ID                              id-at-serviceNumber
}

        -- (90) -- serviceOrAgency ATTRIBUTE
::= {
    WITH SYNTAX                     PrintableString
    EQUALITY MATCHING RULE          caseIgnoreMatch
    SUBSTRINGS MATCHING RULE        caseIgnoreSubstringsMatch
    SINGLE VALUE                    TRUE
    ID                              id-at-serviceOrAgency
}

        -- (91) -- sHD ATTRIBUTE
::= {
    WITH SYNTAX                     PrintableString
    EQUALITY MATCHING RULE          caseIgnoreMatch
    SUBSTRINGS MATCHING RULE        caseIgnoreSubstringsMatch
    ID                              id-at-sHD
}

        -- (92) -- shortTitle ATTRIBUTE
::= {
    WITH SYNTAX                     PrintableString (SIZE (1..55))
    EQUALITY MATCHING RULE          caseIgnoreMatch
    SUBSTRINGS MATCHING RULE        caseIgnoreSubstringsMatch
    SINGLE VALUE                    TRUE
    ID                              id-at-shortTitle
}
```

```
        -- (93) -- sigad ATTRIBUTE
::= {
    WITH SYNTAX                 PrintableString (SIZE (5..8))
    EQUALITY MATCHING RULE      caseIgnoreMatch
    SUBSTRINGS MATCHING RULE    caseIgnoreSubstringsMatch
    SINGLE VALUE                TRUE
    ID                          id-at-sigad
}

        -- (94) -- spot ATTRIBUTE
::= {
    WITH SYNTAX                 PrintableString (SIZE (1..55))
    EQUALITY MATCHING RULE      caseIgnoreMatch
    SUBSTRINGS MATCHING RULE    caseIgnoreSubstringsMatch
    SINGLE VALUE                TRUE
    ID                          id-at-spot
}

        -- (95) -- tARE ATTRIBUTE
::= {
    WITH SYNTAX                 BOOLEAN
    EQUALITY MATCHING RULE      booleanMatch
    SINGLE VALUE                TRUE
    ID                          id-at-tARE
}

        -- (96) -- tCC ATTRIBUTE
::= {
    WITH SYNTAX                 PrintableString
    EQUALITY MATCHING RULE      caseIgnoreMatch
    SINGLE VALUE                TRUE
    ID                          id-at-tCC
}

        -- (97) -- tCCG ATTRIBUTE
::= {
    WITH SYNTAX                 PrintableString
    EQUALITY MATCHING RULE      caseIgnoreMatch
    SUBSTRING MATCHING RULE     caseIgnoreSubstringsMatch
    ID                          id-at-tCCG
}
```

```
        -- (98) -- transferStation ATTRIBUTE
::= {
    WITH SYNTAX                 BOOLEAN
    EQUALITY MATCHING RULE      booleanMatch
    SINGLE VALUE                TRUE
    ID                          id-at-transferStation
}

        -- (99) -- tRC ATTRIBUTE
::= {
    WITH SYNTAX                 PrintableString
    EQUALITY MATCHING RULE      caseIgnoreMatch
    SINGLE VALUE                TRUE
    ID                          id-at-tRC
}

        -- (100) -- usdConversion ATTRIBUTE
::={
    WITH SYNTAX                     DirectoryString
    EQUALITY MATCHING RULE          caseIgnoreMatch
    SUBSTRING MATCHING RULE         caseIgnoreSubstringsMatch
    ID                              id-at-usdConversion
}

    -- d.  collective attributes

        -- (1) -- collective-mhs-or-addresses ATTRIBUTE
::= {
    SUBTYPE OF      mhs-or-addresses
    ID              id-at-collective-mhs-or-addresses
}

        -- (2) -- collectiveMilitaryFacsimileNumber ATTRIBUTE
::= {
    SUBTYPE OF      militaryFacsimileNumber
    ID              id-at-collectiveMilitaryFacsimileNumber
}

        -- (3) -- collectiveMilitaryTelephoneNumber ATTRIBUTE
::= {
    SUBTYPE OF      militaryTelephoneNumber
    ID              id-at-collectiveMilitaryTelephoneNumber
}
```

```
        -- (4) -- collectiveNationality ATTRIBUTE
::= {
    SUBTYPE OF      nationality
    ID              id-at-collectiveNationality
}

        -- (5) -- collectiveSecureFacsimileNumber ATTRIBUTE
::= {
    SUBTYPE OF      secureFacsimileNumber
    ID              id-at-collectiveSecureFacsimileNumber
}

        -- (6) -- collectiveSecureTelephoneNumber ATTRIBUTE
::= {
    SUBTYPE OF      secureTelephoneNumber
    ID              id-at-collectiveSecureTelephoneNumber
}

    -- e.  name forms

        -- (1) -- aCPNetworkEdBNameForm NAME-FORM
::= {
    NAMES           aCPNetworkEdB
    WITH ATTRIBUTES { commonName }
    ID              id-nf-aCPNetworkEdBNameForm
}

        -- (2) -- aCPNetworkInstrEdBNameForm NAME-FORM
::= {
    NAMES           aCPNetworkInstructionsEdB
    WITH ATTRIBUTES { commonName }
    ID              id-nf-aCPNetworkInstrEdBNameForm
}

        -- (3) -- addressListNameForm NAME-FORM
::= {
    NAMES           addressList
    WITH ATTRIBUTES { commonName }
    ID              id-nf-addressList
}
```

```
        -- (4) -- aENameForm NAME-FORM
::= {
    NAMES                   applicationEntity
    WITH ATTRIBUTES         {commonName}
    AND OPTIONALLY          {dnQualifier}
    ID                      id-nf-applicationEntityNameForm
}


        -- (5) -- aliasCNNameForm NAME-FORM
::= {
    NAMES                   { aliasCommonName }
    WITH ATTRIBUTES         { commonName }
    ID                      id-nf-aliasCNNameForm
}


        -- (6) -- aliasOUNameForm NAME-FORM
::= {
    NAMES                   { aliasOrganizationalUnit }
    WITH ATTRIBUTES         { organizationalUnitName }
    ID                      id-nf-aliasOUNameForm
}


        -- (7) -- alternateSpellingPLANameForm NAME-FORM
::= {
    NAMES                   altSpellingACP127
    WITH ATTRIBUTES         { plaNameACP127 }
    ID                      id-nf-alternateSpellingPLANameForm
}


        -- (8) -- cadPLANameForm NAME-FORM
::= {
    NAMES                   cadACP127
    WITH ATTRIBUTES         {plaNameACP127}
    ID                      id-nf-cadPLANameForm
}


        -- (9) -- distributionCodeDescriptionNameForm NAME-FORM
::= {
    NAMES                   { distributionCodeDescription }
    WITH ATTRIBUTES         { commonName }
    ID                      id-nf-distributionCodeDescription
}
```

```
        -- (10) -- dSSCSPLANameForm NAME-FORM
::= {
    NAMES                dSSCSPLA
    WITH ATTRIBUTES      { plaNameACP127 }
    ID                   id-nf-dSSCSPLANameForm
}

        -- (11) -- messagingGatewayNameForm NAME-FORM
::= {
    NAMES                messagingGateway
    WITH ATTRIBUTES      { commonName }
    ID                   id-nf-messagingGateway
}

        -- (12) -- mhs-dLNameForm NAME-FORM
::= {
    NAMES                mhs-distribution-list
    WITH ATTRIBUTES      { commonName }
    ID                   id-nf-mhs-dLNameForm
}

        -- (13) -- mLANameForm NAME-FORM
::= {
    NAMES                mLA
    WITH ATTRIBUTES      { commonName }
    ID                   id-nf-mL ANameForm
}

        -- (14) -- mLAgentNameForm NAME-FORM
::= {
    NAMES                mLAgent
    WITH ATTRIBUTES      { commonName }
    ID                   id-nf-mLAgentNameForm
}

        -- (15) -- mSNameForm NAME-FORM
::= {
    NAMES                mhs-message-store
    WITH ATTRIBUTES      { commonName }
    ID                   id-nf-mS
}
```

```
        -- (16) -- mTANameForm NAME-FORM
::= {
    NAMES               mhs-message-transfer-agent
    WITH ATTRIBUTES     { commonName }
    ID                  id-nf-mTA
}

        -- (17) -- mUANameForm NAME-FORM
::= {
    NAMES               mhs-user-agent
    WITH ATTRIBUTES     { commonName }
    ID                  id-nf-mUA
}

        -- (18) -- networkNameForm NAME-FORM
::= {
    NAMES               network
    WITH ATTRIBUTES     { commonName }
    ID                  id-nf-networkNameForm
}

        -- (19) -- networkInstructionsNameForm NAME-FORM
::= {
    NAMES               networkInstructions
    WITH ATTRIBUTES     { commonName }
    ID                  id-nf-networkInstructionsNameForm
}

        -- (20) -- organizationalPLANameForm NAME-FORM
 ::= {
    NAMES               orgACP127
    WITH ATTRIBUTES     { plaNameACP127 }
    ID                  id-nf-organizationalPLANameForm
}

        -- (21) -- organizationNameForm NAME-FORM
::= {
    NAMES               organization
    WITH ATTRIBUTES     {organizationName}
    AND OPTIONALLY      {dnQualifier}
    ID                  id-nf-qualifiedOrgNameForm
}
```

```
        -- (22) -- orgRNameForm NAME-FORM
::= {
    NAMES               organizationalRole
    WITH ATTRIBUTES     {commonName}
    AND OPTIONALLY      {dnQualifier}
    ID                  id-nf-qualifiedOrgRNameForm
}


        -- (23) -- orgUNameForm NAME-FORM
::= {
    NAMES               organizationalUnit
    WITH ATTRIBUTES     {organizationalUnitName}
    AND OPTIONALLY      {dnQualifier}
    ID                  id-nf-qualifiedOrgUNameForm
}


        -- (24) -- plaCollectiveNameForm NAME-FORM
::= {
    NAMES               plaCollectiveACP127
    WITH ATTRIBUTES     { plaNameACP127 }
    ID                  id-nf-plaCollectiveNameForm
}


        -- (25) -- qualifiedOrgPersonNameForm NAME-FORM
::= {
    NAMES               organizationalPerson
    WITH ATTRIBUTES     {commonName}
    AND OPTIONALLY      {dnQualifier | organizationalUnitName}
    ID                  id-nf-qualifiedOrgPersonNameForm
}


        -- (26) -- releaseAuthorityPersonNameForm NAME-FORM
::= {
    NAMES               releaseAuthorityPerson
    WITH ATTRIBUTES     { releaseAuthorityName }
    ID                  id-nf-releaseAuthorityPersonNameForm
}


        -- (27) -- releaseAuthorityPersonANameForm NAME-FORM
::= {
    NAMES               releaseAuthorityPersonA
    WITH ATTRIBUTES     { releaseAuthorityName }
    ID                  id-nf-releaseAuthorityPersonANameForm
}
```

```
        -- (28) -- routingIndicatorNameForm NAME-FORM
::= {
    NAMES               routingIndicator
    WITH ATTRIBUTES     { rI }
    ID                  id-nf-routingIndicatorNameForm
}


        -- (29) -- sigintPLANameForm NAME-FORM
::= {
    NAMES               sigintPLA
    WITH ATTRIBUTES     { sigad }
    ID                  id-nf-sigintPLANameForm
}


        -- (30) -- sIPLANameForm NAME-FORM
::= {
    NAMES               sIPLA
    WITH ATTRIBUTES     { longTitle }
    ID                  id-nf-sIPLANameForm
}


        -- (31) -- spotPLANameForm NAME-FORM
::= {
    NAMES               spotPLA
    WITH ATTRIBUTES     { spot }
    ID                  id-nf-spotPLANameForm
}


        -- (32) -- taskForcePLANameForm NAME-FORM
::= {
    NAMES               taskForceACP127
    WITH ATTRIBUTES     {plaNameACP127}
    ID                  id-nf-taskForcePLANameForm
}


        -- (33) -- tenantPLANameForm NAME-FORM
::= {
    NAMES               tenantACP127
    WITH ATTRIBUTES     { plaNameACP127 }
    ID                  id-nf-tenantPLANameForm
}
```

```
--  superseded name form
--  uniqueOrgPersonNameForm NAME-FORM
--  ::= {
--  NAMES               organizationalPerson
--  WITH ATTRIBUTES     { commonName }
--  AND OPTIONALLY      { organizationalUnitName |
--                        uniqueIdentifier }
--  ID                  id-nf-uniqueOrgPersonNameForm
--  }


        -- f.  miscellaneous data types

ACPLegacyFormat  ::= INTEGER {
                                    JANAP128(0),
                                    ACP126(1),
                                    DOI103(2),
                                    DOI103Special(3),
                                    ACP127(4),
                                    ACP127Converted(5),
                                    Reserved1(6),       -- hold for ACP127Standard if
                                                        -- needed
                                    ACP127State(7),
                                    ACP127Modified(8),
                                    SOCOMMSpecial(9),
                                    SOCOMMNarrative(10),
                                    Reserved2(11),   -- hold for SOCOMMNarrativeTTY if
                                                     -- needed
                                    SOCOMMNarrativeSpecial(12),
                                    SOCOMMData(13),
                                    SOCOMMInternal(14),
                                    SOCOMMExternal(15) }
                                    -- Note:  Values 32 through 48 are not defined
                                    -- by this ACP and may be used nationally or
                                    -- bilaterally.

ACPTelephoneFaxNumberSyntax ::= PrintableString    -- constructed as defined in
                                                   -- paragraph 27 in this annex

Addressees ::= SEQUENCE OF PrintableString (SIZE (1..55))

Classification ::= ENUMERATED { unmarked(0), unclassified(1), restricted(2),
    confidential(3), secret(4), top-secret(5) }

DistributionCode ::= PrintableString

JPEG ::= OCTET STRING  -- a JPEG image

MonthlyUKMs ::= SIGNED { SEQUENCE OF UKMEntry }

Remarks ::= SEQUENCE OF PrintableString
```

```
RIParameters ::= SET {
    rI              [0] PrintableString,
    rIType          [1] ENUMERATED { normal(0), off-line(1), partTimeTerminal(2) },
    minimize        [2] BOOLEAN,  -- not used any more --
    sHD             [3] PrintableString,
    classification [4] Classification
}

UKMEntry ::= SEQUENCE {
    tag     PairwiseTag,
    ukm     OCTET STRING
}


        -- g.  object identifiers

ID ::= OBJECT IDENTIFIER

ds ID ::= { joint-iso-ccitt(2) country(16) us(840) organization(1) gov(101) dod(2) ds(2) }

--categories of information objects--

id-module      ID ::= {id-ds 0}
id-attributeType  ID ::= {id-ds 1}
id-objectClass    ID ::= {id-ds 3}
id-nameForm       ID ::= {id-ds 4}
id-gatewayType    ID ::= {id-ds 5 }

-- synonyms --

id-at    ID ::= { id-ds attributeType(1) }
id-gt    ID ::= { id-ds gatewayType(5) }
id-nf    ID ::= { id-ds nameForm(4) }
id-oc    ID ::= { id-ds objectClass(3) }

-- Attributes registered in  SDN.700 , which is the definitive assignment, and
-- repeated here

id-at-alid  -- [id-mlid] --    ID ::= { 2 16 840 1 101 2 1 5 14 }
id-at-janUKMs     ID ::= { 2 16 840 1 101 2 1 5 20 }
id-at-febUKMs     ID ::= { 2 16 840 1 101 2 1 5 21 }
id-at-marUKMs     ID ::= { 2 16 840 1 101 2 1 5 22 }
id-at-aprUKMs     ID ::= { 2 16 840 1 101 2 1 5 23 }
id-at-mayUKMs     ID ::= { 2 16 840 1 101 2 1 5 24 }
id-at-junUKMs     ID ::= { 2 16 840 1 101 2 1 5 25 }
id-at-julUKMs     ID ::= { 2 16 840 1 101 2 1 5 26 }
id-at-augUKMs     ID ::= { 2 16 840 1 101 2 1 5 27 }
id-at-sepUKMs     ID ::= { 2 16 840 1 101 2 1 5 28 }
id-at-octUKMs     ID ::= { 2 16 840 1 101 2 1 5 29 }
id-at-novUKMs     ID ::= { 2 16 840 1 101 2 1 5 30 }
```

```
id-at-decUKMs    ID ::= { 2 16 840 1 101 2 1 5 31 }
id-at-aLExemptedAddressProcessor  ID ::= { 2 16 840 1 101 2 1 5 47 }
--     [id-mlExemptedAddressProcessor]

-- Attributes registered in RFC 1274 --

-- buildingName   ID ::=   { 0 9 2342 192003000 100 1 48 } --
-- host ID ::=   { 0 9 2342 192003000 100 1 9 } --
-- rfc822Mailbox  ID ::=   { 0 9 2342 192003000 100 1 3 } --
-- roomNumber   ID ::=   { 0 9 2342 192003000 100 1 6 } --

-- ACP 133 attributes --

id-at-alternateRecipient ID ::=   { id-at 3 }
id-at-associatedOrganization   ID ::=   { id-at 4 }
id-at-associatedPLA      ID ::=   { id-at 6 }
id-at-releaseAuthorityName      ID ::=   { id-at 45 }
id-at-actionAddressees ID ::=   { id-at 46 }
id-at-additionalAddressees      ID ::=   { id-at 47 }
id-at-additionalSecondPartyAddressees  ID ::=   { id-at 48 }
id-at-aliasPointer     ID ::=   { id-at 49 }
id-at-allowableOriginators  ID ::=   { id-at 50 }
id-at-cognizantAuthority     ID ::=   { id-at 51 }
id-at-community  ID ::=   { id-at 52 }
id-at-accountingCode    ID ::=   { id-at 53 }
id-at-dualRoute   ID ::=   { id-at 54 }
id-at-effectiveDate    ID ::=   { id-at 55 }
id-at-entryClassification      ID ::=   { id-at 56 }
id-at-expirationDate ID ::=   { id-at 57 }
id-at-hostOrgACP127     ID ::=   { id-at 58 }
id-at-infoAddressees     ID ::=   { id-at 59 }
id-at-lastRecapDate  ID ::=   { id-at 60 }
id-at-listPointer   ID ::=   { id-at 61 }
id-at-lmf    ID ::=   { id-at 62 }
id-at-longTitle     ID ::=   { id-at 63 }
id-at-minimize     ID ::=   { id-at 64 }
id-at-minimizeOverride  ID ::=   { id-at 65 }
id-at-nameClassification     ID ::=   { id-at 67 }
id-at-nationality   ID ::=   { id-at 68 }
id-at-collectiveNationality    ID ::=   { id-at 68 collective(1) }
id-at-transferStation ID ::=   { id-at 69 }
id-at-plaNameACP127    ID ::=   { id-at 70 }
id-at-plaAddressees      ID ::=   { id-at 71 }
id-at-plaReplace  ID ::=   { id-at 72 }
id-at-primarySpellingACP127    ID ::=   { id-at 73 }
id-at-publish   ID ::=   { id-at 74 }
id-at-recapDueDate   ID ::=   { id-at 75 }
id-at-remarks      ID ::=   { id-at 76 }
id-at-rl      ID ::=   { id-at 77 }
id-at-rlClassification      ID ::=   { id-at 78 }
id-at-rlInfo     ID ::=   { id-at 79 }
```

id-at-secondPartyAddressees ID ::= { id-at 80 }
id-at-section ID ::= { id-at 81 }
id-at-serviceOrAgency ID ::= { id-at 82 }
id-at-sHD ID ::= { id-at 83 }
id-at-shortTitle ID ::= { id-at 84 }
id-at-sigad ID ::= { id-at 85 }
id-at-spot ID ::= { id-at 86 }
id-at-tARE ID ::= { id-at 87 }
id-at-aCPMobileTelephoneNumber ID ::= { id-at 94 }
id-at-aCPPagerTelephoneNumber ID ::= { id-at 95 }
id-at-tCC ID ::= { id-at 96 }
id-at-tRC ID ::= { id-at 97 }
id-at-distributionCodeAction ID ::= { id-at 104 }
id-at-distributionCodeInfo ID ::= { id-at 105 }
id-at-accessCodes ID ::= { id-at 106 }
id-at-accessSchema ID ::= { id-at 107 }
id-at-aCPPreferredDelivery ID ::= { id-at 108 }
id-at-aCPTelephoneFaxNumber ID ::= { id-at 109 }
id-at-administrator ID ::= { id-at 110 }
id-at-aigsExpanded ID ::= { id-at 111 }
id-at-aLType ID ::= { id-at 112 }
id-at-associatedAL ID ::= { id-at 113 }
id-at-copyMember ID ::= { id-at 114 }
id-at-gatewayType ID ::= { id-at 115 }
id-at-ghpType ID ::= { id-at 116 }
id-at-guard ID ::= { id-at 117 }
id-at-mailDomains ID ::= { id-at 118 }
id-at-militaryFacsimileNumber ID ::= { id-at 119 }
id-at-collectiveMilitaryFacsimileNumber ID ::= { id-at 119 collective(1) }
id-at-militaryTelephoneNumber ID ::= { id-at 120 }
id-at-collectiveMilitaryTelephoneNumber ID ::= { id-at 120 collective(1) }
id-at-networkDN ID ::= { id-at 121 }
id-at-networkSchema ID ::= { id-at 122 }
id-at-onSupported ID ::= { id-at 123 }
id-at-operationName ID ::= { id-at 124 }
id-at-positionNumber ID ::= { id-at 125 }
id-at-proprietaryMailboxes ID ::= { id-at 126 }
id-at-secureFacsimileNumber ID ::= { id-at 127 }
id-at-collectiveSecureFacsimileNumber ID ::= { id-at 127 collective(1) }
id-at-secureTelephoneNumber ID ::= { id-at 128 }
id-at-collectiveSecureTelephoneNumber ID ::= { id-at 128 collective(1) }
id-at-serviceNumberID ::= { id-at 129 }
id-at-rank ID ::= { id-at 133 }
id-at-misc-collectives ID ::= { id-at 134 }
id-at-collective-mhs-or-addresses ID ::= { id-at 134 collective-mhs-or-addresses(1) }
id-at-aLReceiptPolicy ID ::= { id-at 135 }
id-at-plasServed ID ::= { id-at 138 }
id-at-deployed ID ::= { id-at 139}
id-at-garrisonID ::= { id-at 140}
id-at-aCPLegacyFormat ID ::= { id-at 142 }
id-at-adminConversion ID ::= { id-at 143}

```
id-at-tCCG     ID ::=  { id-at 144 }
id-at-usdConversionID ::=  { id-at 145}
id-at-aCPNetwAccessSchemaEdB ID ::=  { id-at 146 }
id-at-aCPNetworkSchemaEdB  ID ::=  { id-at 147 }

-- ACP 133 Name Forms --

id-nf-alternateSpellingPLANameForm ID ::=  { id-nf 4 }
id-nf-cadPLANameForm      ID ::=  { id-nf 6 }
id-nf-mLANameForm     ID ::=  { id-nf 9 }
id-nf-organizationalPLANameForm     ID ::=  { id-nf 12 }
id-nf-plaCollectiveNameForm   ID ::=  { id-nf 13 }
id-nf-routingIndicatorNameForm   ID ::=  { id-nf 15 }
id-nf-sigintPLANameForm   ID ::=  { id-nf 16 }
id-nf-sIPLANameForm   ID ::=  { id-nf 17 }
id-nf-spotPLANameForm    ID ::=  { id-nf 18 }
id-nf-taskForcePLANameForm ID ::=  { id-nf 19 }
id-nf-tenantPLANameForm  ID ::=  { id-nf 20 }
id-nf-aliasCNNameForm     ID ::=  { id-nf 21 }
id-nf-aliasOUNameForm     ID ::=  { id-nf 22 }
id-nf-distributionCodeDescription ID ::=  { id-nf 23 }
id-nf-mS   ID ::=  { id-nf 24 }
id-nf-mTA ID ::=  { id-nf 25 }
id-nf-mUA      ID ::=  { id-nf 26 }
id-nf-addressList     ID ::=  { id-nf 27 }
id-nf-messagingGateway    ID ::=  { id-nf 28 }
id-nf-mhs-dLNameForm      ID ::=  { id-nf 29 }
id-nf-networkNameForm     ID ::=  { id-nf 30 }
id-nf-networkInstructionsNameForm   ID ::=  { id-nf 31 }
id-nf-releaseAuthorityPersonNameForm  ID ::=  { id-nf 32 }
--  id-nf-uniqueOrgPersonNameForm  ID ::=  { id-nf 33 } (superseded)
id-nf-applicationEntityNameForm  ID ::=  { id-nf 34 }
id-nf-qualifiedOrgNameForm   ID ::=  { id-nf 35 }
id-nf-qualifiedOrgPersonNameForm   ID ::=  { id-nf 36 }
id-nf-qualifiedOrgRNameForm ID ::=  { id-nf 37 }
id-nf-qualifiedOrgUNameForm ID ::=  { id-nf 38 }
id-nf-releaseAuthorityPersonANameForm     ID ::=  { id-nf 39 }
id-nf-mLAgentNameForm   ID ::=  { id-nf 40 }
id-nf-dSSCSPLANameFormID ::=  { id-nf 41 }
id-nf-aCPNetworkEdBNameForm  ID ::=  { id-nf 42 }
id-nf-aCPNetworkInstrEdBNameFormID ::=  { id-nf 43 }

-- Object classes registered in SDN.700 , which is the definitive assignment,
-- and repeated here

id-oc-secure-user     ID ::=  { 2 16 840 1 101 2 1 4 13 }
id-oc-ukms     ID ::=  { 2 16 840 1 101 2 1 4 16 }
```

```
-- ACP 133 object classes --

id-oc-plaData      ID ::=  { id-oc 26 }
id-oc-cadACP127    ID ::=  { id-oc 28 }
id-oc-mLA     ID ::=  { id-oc 31 }
id-oc-orgACP127    ID ::=  { id-oc 34 }
id-oc-plaCollectiveACP127  ID ::=  { id-oc 35 }
id-oc-routingIndicator   ID ::=  { id-oc 37 }
id-oc-sigintPLA   ID ::=  { id-oc 38 }
id-oc-sIPLA   ID ::=  { id-oc 39 }
id-oc-spotPLA     ID ::=  { id-oc 40 }
id-oc-taskForceACP127      ID ::=  { id-oc 41 }
id-oc-tenantACP127 ID ::=  { id-oc 42 }
id-oc-plaACP127    ID ::=  { id-oc 47 }
id-oc-aliasCommonName    ID ::=  { id-oc 52 }
id-oc-aliasOrganizationalUnit   ID ::=  { id-oc 53 }
id-oc-distributionCodesHandled    ID ::=  { id-oc 54 }
id-oc-distributionCodeDescription     ID ::=  { id-oc 55 }
id-oc-plaUser      ID ::=  { id-oc 56 }
id-oc-addressList     ID ::=  { id-oc 57 }
id-oc-altSpellingACP127     ID ::=  { id-oc 58 }
id-oc-messagingGateway    ID ::=  { id-oc 59 }
id-oc-network     ID ::=  { id-oc 60 }
id-oc-networkInstructions  ID ::=  { id-oc 61 }
id-oc-otherContactInformation ID ::=  { id-oc 62 }
id-oc-releaseAuthorityPerson  ID ::=  { id-oc 63 }
id-oc-mLAgent    ID ::=  { id-oc 64 }
id-oc-releaseAuthorityPersonAID ::=  { id-oc 65 }
id-oc-securePkiUserID ::=  { id-oc 66 }
id-oc-dSSCSPLAID ::=  { id-oc 67 }
id-oc-aCPNetworkEdB   ID ::=  { id-oc 68 }
id-oc-aCPNetworkInstructionsEdBID ::=  { id-oc 69 }

--gateway types--

acp120-acp127    ID ::=  { id-gt 0 }
acp120-janap128 ID ::=  { id-gt 1 }
acp120-mhs   ID ::=  { id-gt 2 }
acp120-mmhs      ID ::=  { id-gt 3 }
acp120-rfc822      ID ::=  { id-gt 4 }
boundaryMTA    ID ::=  { id-gt 5 }
mmhs-mhs    ID ::=  { id-gt 6 }
mmhs-rfc822 ID ::=  { id-gt 7 }
mta-acp127    ID ::=  { id-gt 8 }

END  -- Common Content --
```

208. Useful Attributes ASN.1 Definitions

The following ASN.1 module specifies attributes and their object identifiers that are useful to more than one of the Allies, but are not part of the Allied Directory schema. This module imports only the data types used by the included definitions. Useful attributes shall not be replicated unless specific bi-lateral arrangements are made for their support on both the supplier and consumer systems.

209. Useful Attributes Module

```
ACP133UsefulAttributes { joint-iso-ccitt(2) country(16) us(840) organization(1) gov(101)
dod(2) ds(2) module(0) usefulAttributes(3) editionA(2) }

DEFINITIONS ::=
BEGIN

IMPORTS

ATTRIBUTE
    FROM InformationFramework { joint-iso-ccitt ds(5) modules(1)
            informationFramework(1) 2 }

caseIgnoreMatch, caseIgnoreSubstringsMatch, DirectoryString, postalAddress
    FROM SelectedAttributeTypes { joint-iso-ccitt ds(5) module(1) usefulDefinitions(0) 2 }

id-at, JPEG
    FROM ACP133CommonContent { joint-iso-ccitt(2) country(16) us(840) organization(1)
            gov(101) dod(2) ds(2) module(0) 2 2 }

;  -- end of IMPORTS


        -- a. -- hoursOfOperation ATTRIBUTE
::= {
    WITH SYNTAX                     DirectoryString
    EQUALITY MATCHING RULE          caseIgnoreMatch
    SUBSTRINGS MATCHING RULE        caseIgnoreSubstringsMatch
    ID                              id-at-hoursOfOperation
}


        -- b. -- jpegPhoto ATTRIBUTE
::= {
    WITH SYNTAX    OCTET STRINGJPEG  -- values of the string are
                                     -- JPEG- formatted (JFIF) photographs
    ID             id-at-jpegPhoto
}
```

```
        -- c. -- militaryPostalAddress ATTRIBUTE
::= {
    SUBTYPE OF              postalAddress
    ID                      id-at-militaryPostalAddress
}


        -- d. -- visitorAddress ATTRIBUTE
::= {
    SUBTYPE OF              postalAddress
    ID                      id-at-visitorAddress
}


        -- e. -- collectiveMilitaryPostalAddress ATTRIBUTE
::= {
    SUBTYPE OF          militaryPostalAddress
    ID                  id-at-collectiveMilitaryPostalAddress
}


        -- f. -- collectiveVisitorAddress ATTRIBUTE
::= {
    SUBTYPE OF          visitorAddress
    ID                  id-at-collectiveVisitorAddress
}

id-at-hoursOfOperation ID ::=  { id-at 130 }
id-at-jpegPhoto   ID ::=  { 0 9 2342 19200300 100 1 60 }
id-at-militaryPostalAddressID ::=  { id-at 131 }
id-at-collectiveMilitaryPostalAddress  ID ::=  { id-at 131 collective(1) }
id-at-visitorAddress ID ::=  { id-at 132 }
id-at-collectiveVisitorAddress  ID ::=  { id-at 132 collective(1) }

END  -- Useful Attributes --
```

ANNEX C

DIRECTORY PROFILES

1. General

This annex describes the ISPs that have been developed for the directory standards. This annex has been included in ACP 133 as background information on the functional profiles that provide the basis for the ACP 133 Profiles in Annex D. All profile requirements for the Allied Directory System are contained in Annex D.

a. Functional profiles are used to define the detailed capabilities of directory products. They are developed from the Directory Standards, in particular, the Protocol Implementation Conformance Statement (PICS) proformas, and refine these specifications by making choices where alternatives are defined and by setting specific values for parameters of directory protocol operation or directory information definition. For example, a profile could be written for a DUA product that limits the operations used to Bind, Unbind, and Read and restricts the attributes that are read to a certain set.

b. The directory functional profiles fall into two major categories: Application Profiles and Interchange Format and Representation Profiles. These categories are defined in ISO/IEC Technical Report (TR) 10000 which defines and classifies functional profiles for OSI. For the Directory, protocols and operations are the subjects of Application Profiles, and generic and application-specific schema are the subjects of Interchange Format and Representation Profiles. Within these two categories, the capabilities of the standard directory have been divided into several subject areas for profiling. Each subject area or class may be broken down further into functional profiles. Figure C-1 shows the directory functional profiles and the label applied to each one through the identification scheme (taxonomy) contained in TR 10000.

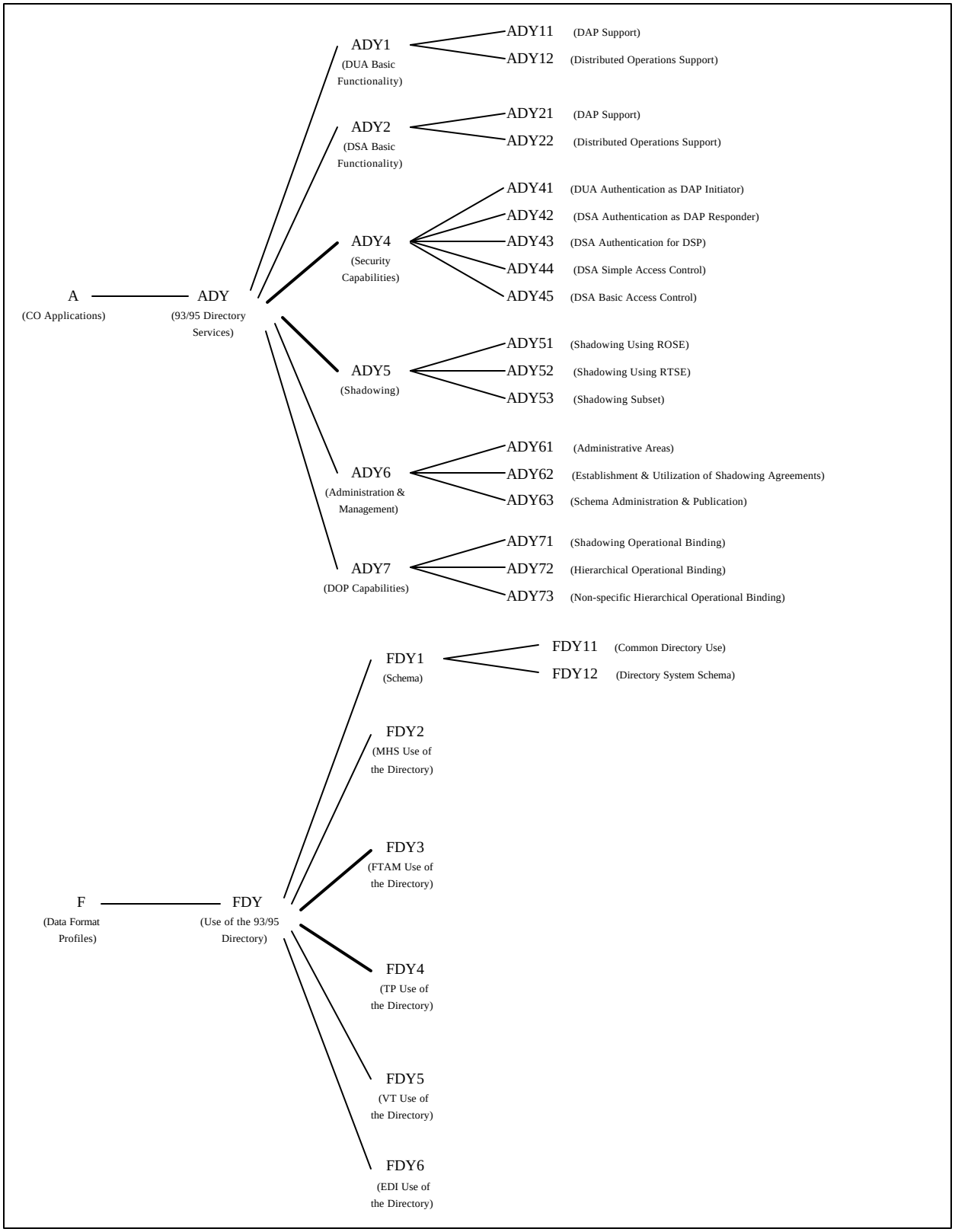

Figure C-1

Taxonomy of Directory Functional Profiles

c. The classes of directory profiles are:

- ADY1 - DUA Basic Functionality
- ADY2 - DSA Basic Functionality
- ADY4 - Security Capabilities
- ADY5 - Shadowing Capabilities
- ADY6 - Directory Administration and Management
- ADY7 - DOP Capabilities
- FDY1 - Schema
- FDY2 - MHS Use of the Directory
- FDY3 - FTAM Use of the Directory
- FDY4 - TP Use of the Directory
- FDY5 - VT Use of the Directory
- FDY6 - EDI Use of the Directory

2. Directory Application Profiles

a. ADY1 - DUA Basic Functionality

The ADY1 class of profiles defines the basic behavior of a DUA in its communication with a DSA. It does not define the DUA's interaction with the user. There are two functional profiles in this class:

- ADY11 - DUA Support of Directory Access Protocol
- ADY12 - DUA Support of Distributed Operations

(1) The ADY11 profile defines the behavior of a DUA regarding the operation of the DAP when interacting with a single DSA to perform a single user request. It covers the DUA performing the initiator role of DAP, invoking an operation on a DSA, and receiving a result or error response (see Figure C-2). ADY11 specifies constraints on the use of a DSA by a DUA to interwork with the Directory services.

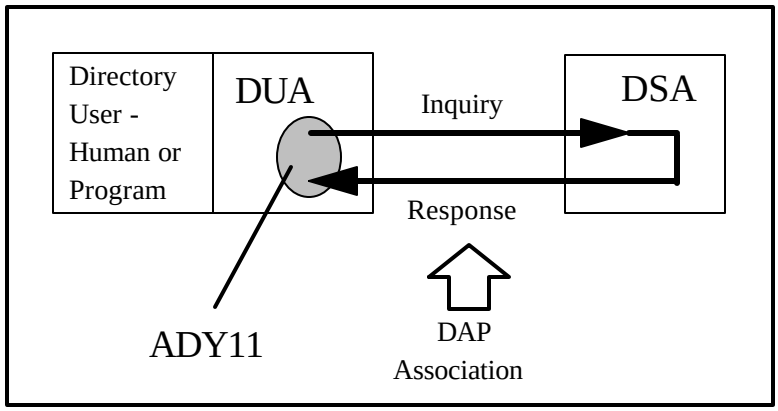

Figure C-2

ADY11 Applicability

(2) The ADY12 profile defines the behavior of a DUA, regarding the operation of DAP, when performing multiple interactions with multiple DSAs to perform a single user request. That is ADY12 profiles the behavior of a DUA when Referrals or Search Continuation References are used by the Directory. A DUA creates an association to a DSA of its choice, and requests an operation. The DSA may return a referral instead of a result, or the result may contain continuation references. The latter occur in the case of List or Search operations in which the DSA is unwilling or unable to complete the search, but is able to advise which other DSAs may be able to assist. The DUA then associates with the recommended DSA to continue the operation. See Figure C-3.

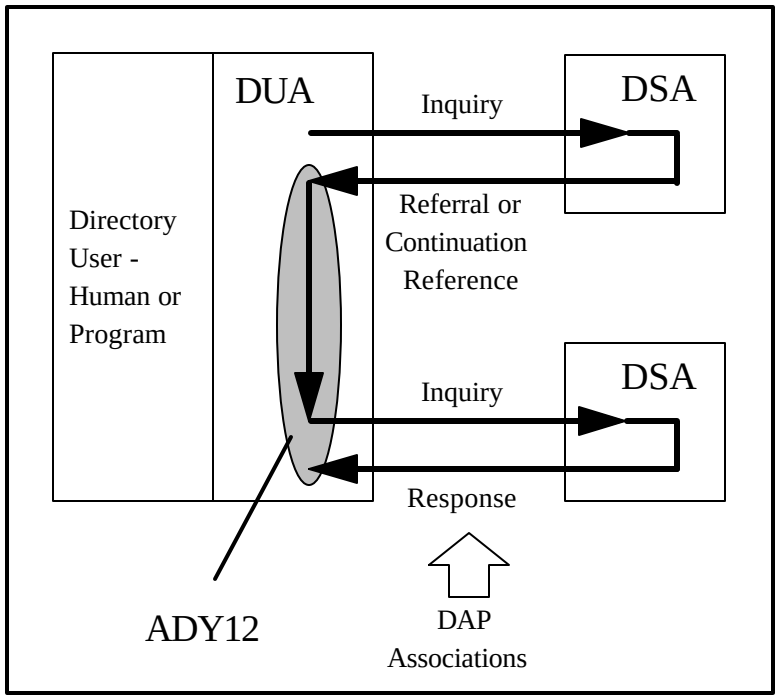

Figure C-3

Applicability of ADY12

b. ADY2 - DSA Basic Functionality

The ADY2 class of profiles defines the basic behavior of a DSA in its communication with DUAs and other DSAs. There are two functional profiles in this class:

- ADY21 - DSA Support of Directory Access
- ADY22 - DSA Support of Distributed Operations

(1) The ADY21 profile defines the behavior of a DSA regarding the operation of the DAP for communicating with a DUA. It covers the DSA performing the responder role of DAP, receiving the invocation of an operation from a DSA, and responding with a result or error response (see Figure C-4). ADY21 defines capabilities and constraints on support for DAP by DSAs so that DUAs are able to interwork with the Directory.

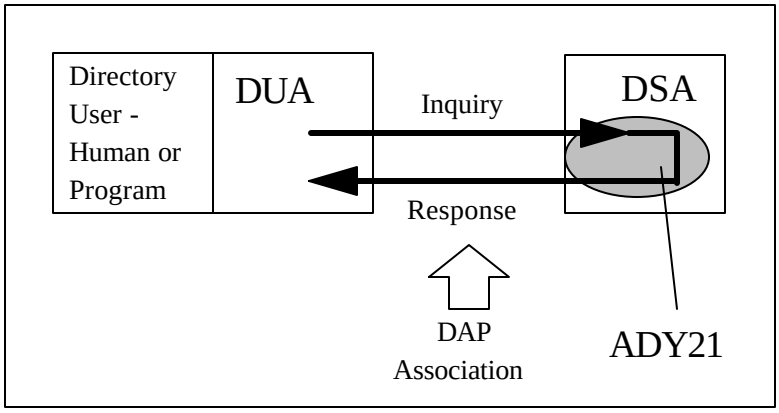

Figure C-4

ADY21 Applicability

(2) The ADY22 profile defines the behavior of a DSA regarding the operation of the DSP when communicating with another DSA, and it defines the coordination of a DSA communication across several associations to perform a particular distributed operation (see Figure C-5). It covers the DSA performing the invoker role of DSP, the performer role, or both; DSAs as users (over DAP or DSP) of Referrals and Continuation references; and DSAs as users of Hierarchical Operational Bindings (HOBs) and of Shadow Operational Bindings in so far as they affect distributed operations using DSP. ADY22 ensures that DSAs will be able to interwork within the Directory in two respects:

- Correct protocol behavior
- Correct behavior in respect of the role that each DSA has to play in respect of Distributed Operations

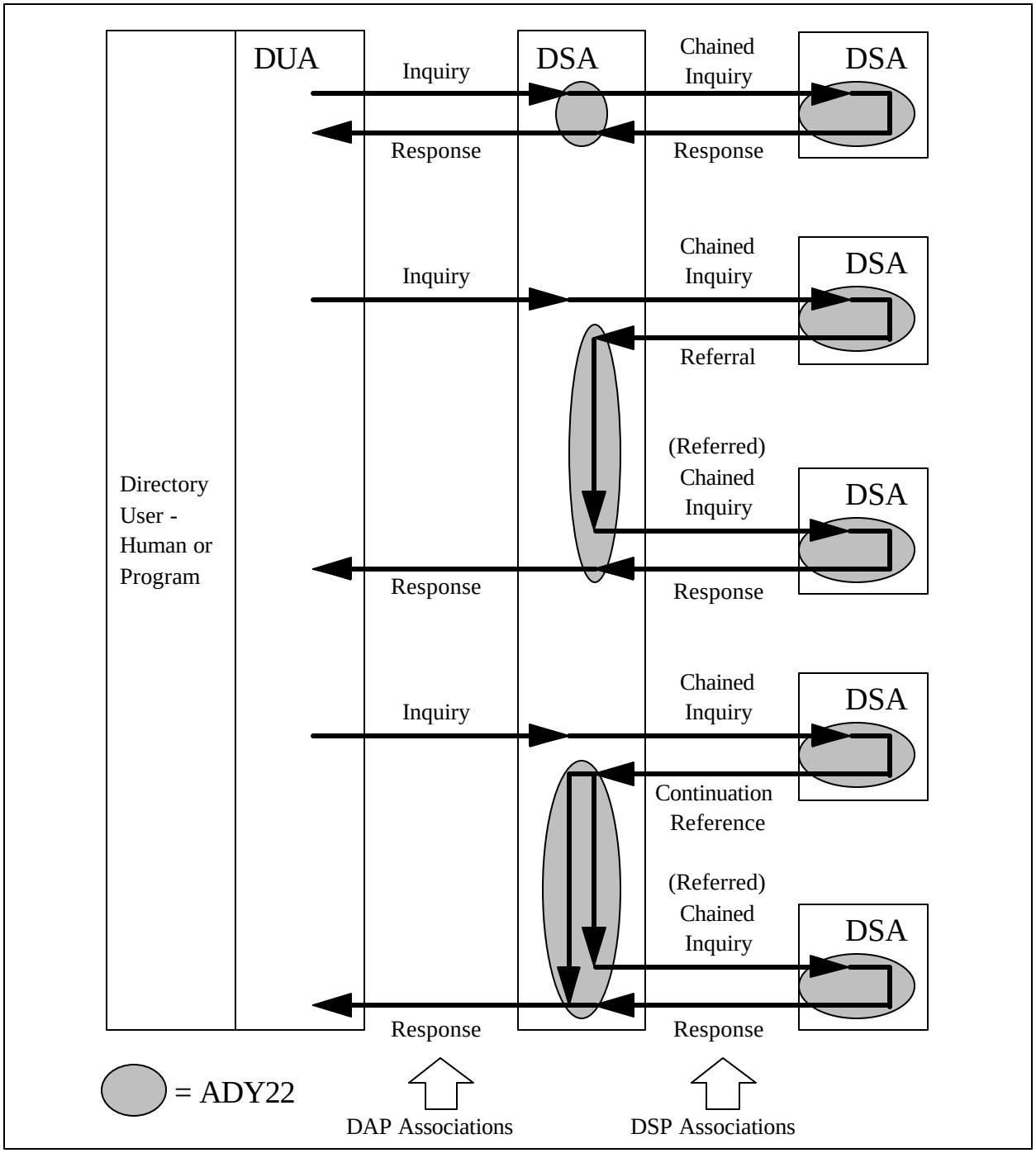

Figure C-5

ADY22 Applicability

c. ADY4 - Security Capabilities

The ADY4 class of profiles defines the behavior of directory components in supporting various security features and degrees of security. There are five functional profiles in this class:

- ADY41 - DUA Authentication as DAP Initiator
- ADY42 - DSA Authentication as DAP Responder
- ADY43 - DSA to DSA Authentication
- ADY44 - DSA Simple Access Control
- ADY45 - DSA Basic Access Control

(1) The ADY41 profile specifies the manner in which a DUA behaves when authenticating a DSA and authenticating itself to a DSA using simple protected authentication or strong authentication as a DAP Initiator. It augments the ADY11 requirements with DUA-specific use of authentication beyond simple unprotected binds and use of digitally signed operations (see Figure C-6). ADY41 includes use of different levels of authentication, and of different security infrastructures, e.g., support of hierarchical/non-hierarchical CA structures. In addition, ADY41 covers actions by the DUA on handling (i.e., validating or not) credentials returned by the DSA, the use of two-way strong authentication, and digitally signed operations.

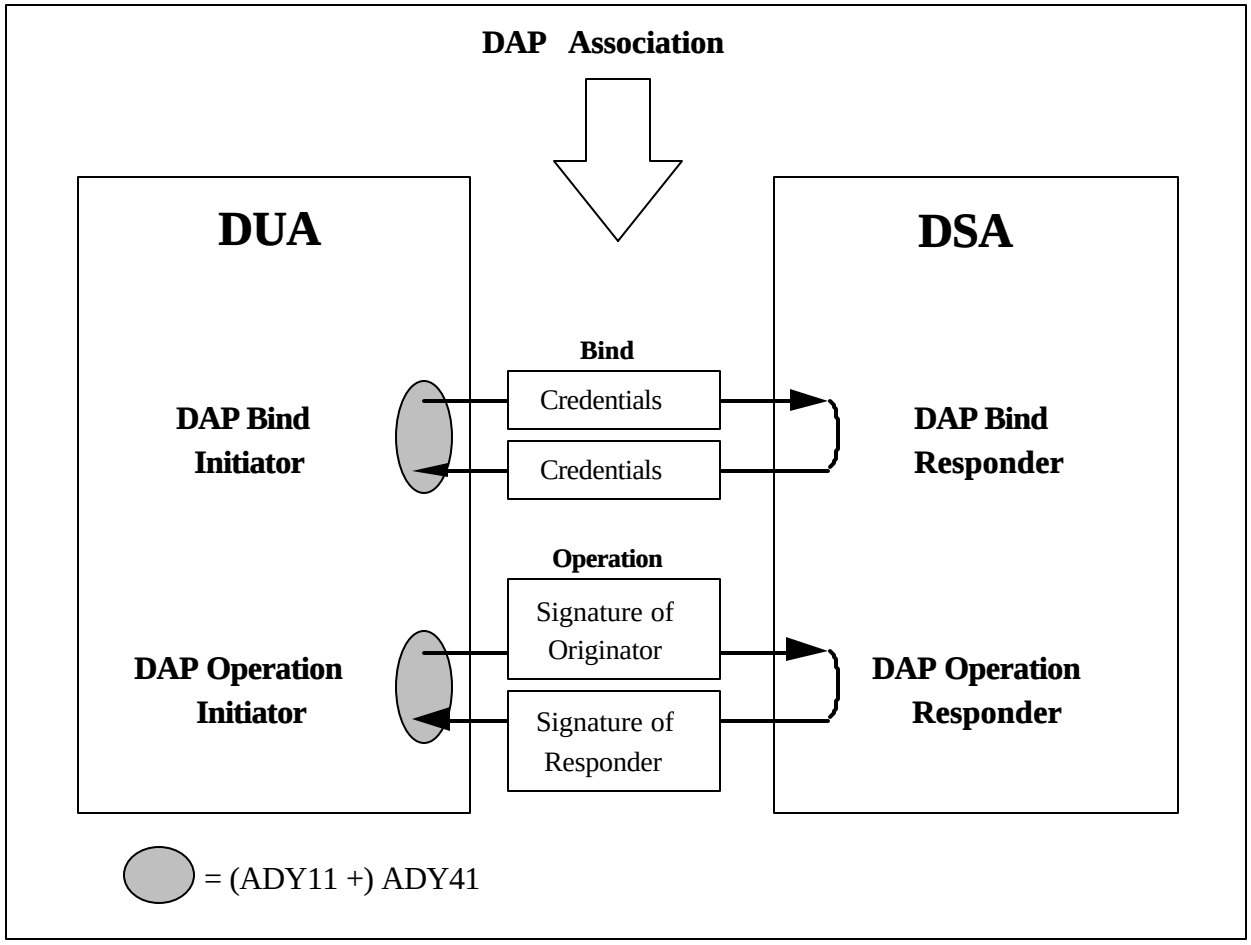

Figure C-6

ADY41 Applicability

(2) The ADY42 profile specifies the manner in which a DSA behaves when authenticating a DUA and authenticating itself to a DUA using simple protected authentication or strong authentication as a DAP Responder. It augments the ADY21 requirements with DUA-specific use of authentication beyond simple unprotected binds and use of digitally signed operations (see Figure C-7). ADY42 includes use of different levels of authentication, and of different security infrastructures, e.g., support of hierarchical/non-hierarchical CA structures. In addition, ADY42 covers actions by the DSA on handling (i.e., validating or not) credentials sent by the DUA, the use of two-way strong authentication, procedures for distributed authentication, and digitally signed operations.

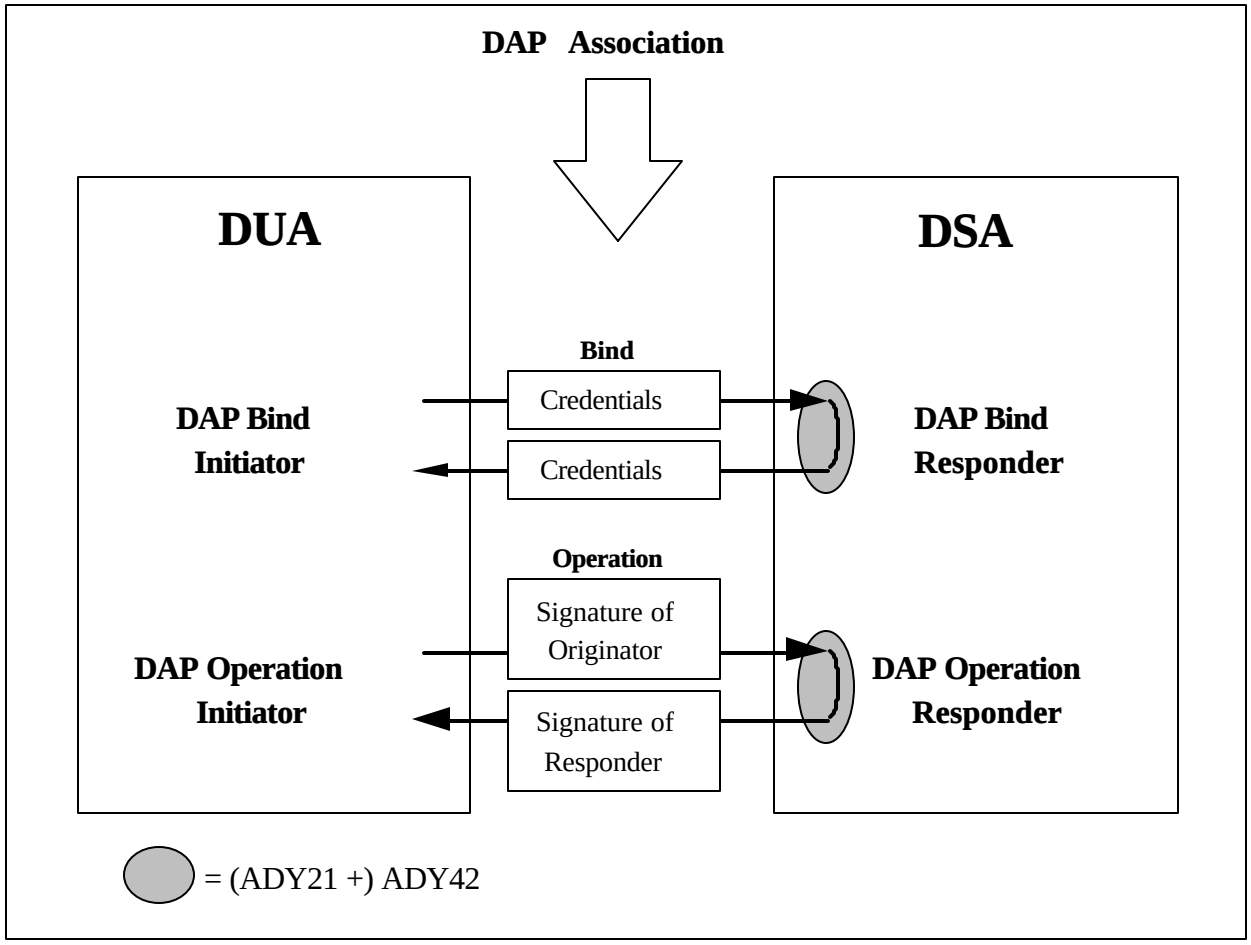

Figure C-7

ADY42 Applicability

(3) The ADY43 profile is titled DSA to DSA Authentication. However, this is different from the title given in TR 10000 (DSA Authentication for DSP) and reflects a broadening of scope since the Directory profiles taxonomy was formulated. ADY43 covers the use of authentication beyond simple unprotected password for the purpose of mutual authentication of DSAs in establishment of DSP, DISP, and DOP associations. It includes use of 2 x one-way strong authentication, two-way strong authentication and the use of security-related protocol elements. ADY43 also covers digitally signed DSP and DISP operations. ADY43 profiles the behavior of a DSA in combining signed uncorrelated list and search information as returned by DSP return results and the use of the originator element to convey information about the originator of the DAP operation that is the cause of the DSP operations. See Figure C-8.

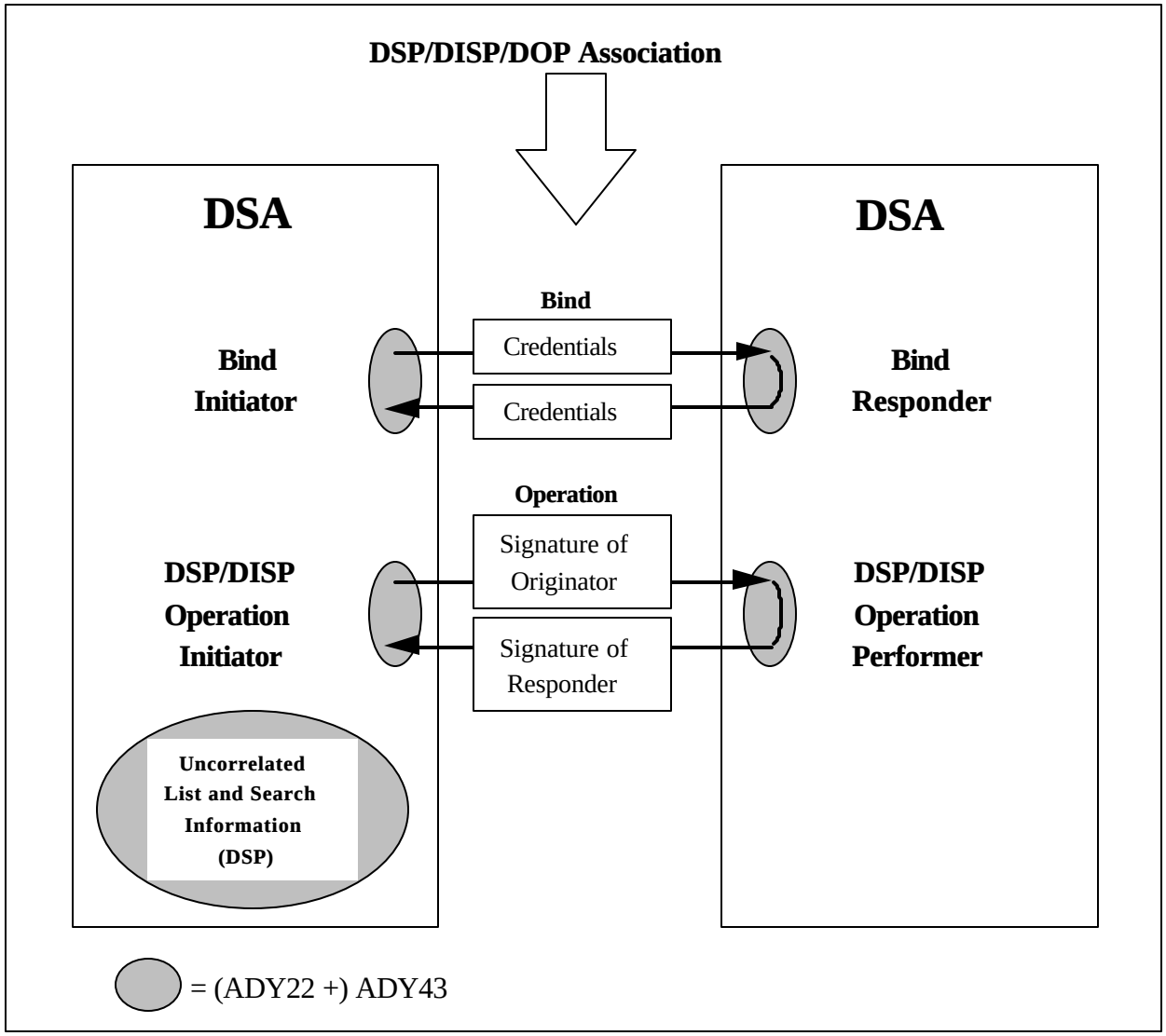

Figure C-8

ADY43 Applicability

(4) Although ADY44 is defined in TR 10000 to be a separate profile from ADY45, ADY44 has been absorbed into ADY45, because of the large amount of commonality. The ADY44 profile specifies the manner in which DSAs perform Simplified Access Control (SAC) by supporting Access Control Specific Administrative Areas, Protected Item categories, User Classes, and GrantAndDenials facilities as defined in subentries. ADY44 defines capabilities and constraints of DSAs supporting SAC. SAC is performed by DSAs to determine if a requestor is allowed access to the requested information stored in the DSA. The DSA compares a presented DAP or DSP request for information to the stored information's ACIItem, and then performs an access control decision to determine whether permission to access the information should be granted or denied to the requestor (see Figure C-9). SAC is relevant both when the DSA is acting as responder to DAP requests from a DUA and as responder to DSP operations from a peer DSA. In SAC, access control decisions are

made on the basis of ACIItem values of prescriptiveACI and subentryACI operational attributes, which must be located at a single Administrative Point or its immediate subentries.

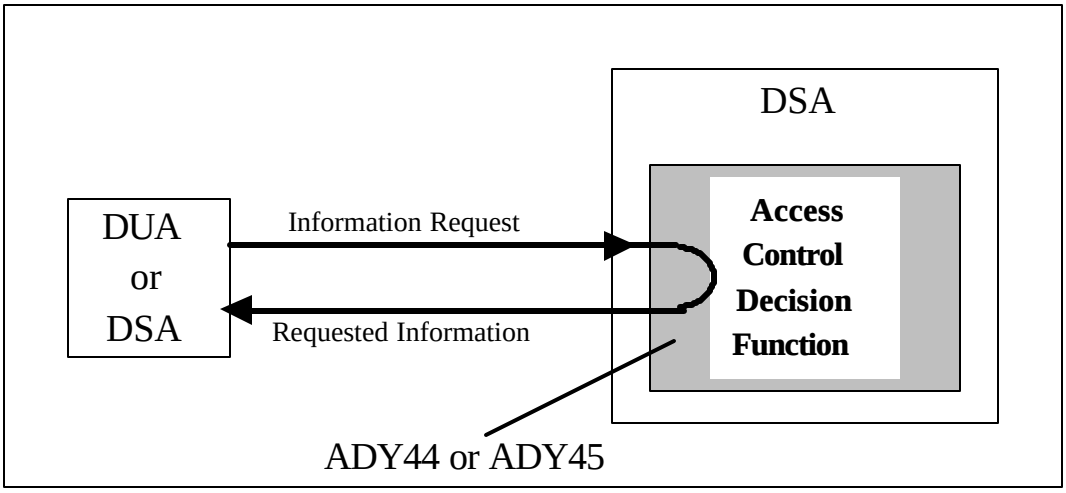

Figure C-9

ADY44 or ADY45 Applicability

(5) The ADY45 profile specifies the manner in which DSAs BAC by supporting Access Control Specific Administrative Areas and Inner Administrative Areas, Protected Item categories, User Classes, and GrantAndDenials facilities as defined in subentries and/or entries. ADY45 defines capabilities and constraints of DSAs supporting BAC. BAC is performed by DSAs to determine if a requestor is allowed access to the requested information stored in the DSA. The DSA compares a presented DAP or DSP request for information to the stored information's ACIItem, and then performs an access control decision to determine whether permission to access the information should be granted or denied to the requestor (see Figure C-9). BAC is relevant both when the DSA is acting as responder to DAP requests from a DUA and as responder to DSP operations from a peer DSA. In BAC, access control decisions are made on the basis of ACIItem values of prescriptiveACI, subentryACI, and entryACI operational attributes. PrescriptiveACI and subentryACI are associated with the administrative point of an Access Control Specific Area or an Access Control Inner Area. EntryACI is associated with a particular entry.

d. ADY5 - Shadowing Capabilities

The ADY5 class of profiles covers the protocol and functional aspects related to Directory shadowing. Operational and procedural aspects of shadowing are covered in ADY22 and ADY62. There are three functional profiles in this class:

- ADY51 - Shadowing Using ROSE
- ADY52 - Shadowing Using RTSE
- ADY53 - Shadowing Subset

(1) The ADY51 profile defines a set of capabilities and constraints on support of DISP by DSAs when operating DISP over the Remote Operations Service Element (ROSE). ADY51 specifies a level of DISP capability such that DSAs shall be capable of establishing and maintaining DISP associations over ROSE together in a consistent manner. ADY51 covers primary and secondary shadowing and the consumer and supplier DSA roles.

(2) The ADY52 profile defines a set of capabilities and constraints on support of DISP by DSAs when operating DISP over the Reliable Transfer Service Element (RTSE). Both the consumer and supplier roles and the 'push' and 'pull' models are covered. In addition, error handling and recovery capabilities are also profiled.

(3) The ADY53 profile defines an incremental set of Directory shadowing capabilities that can be provided by a DSA implementation. These functional capabilities are related specifically to the level of refinement supported for the definition of a unit of replication. The capability to support overlapped units of replications is also incorporated. Both the DSA shadow supplier and consumer roles are covered.

e. ADY6 - Directory Administration and Management

The ADY6 class of profiles is aimed at regulating the policies and procedures that administrations shall define in order to make the Directory work smoothly in its environment. This is achieved by describing the various subjects for coordination within and between administrative areas and methods for the coordination based on derived policies. There are three functional profiles in this class:

- ADY61 - Administrative Areas
- ADY62 - Establishment and Utilization of Shadowing Agreements
- ADY63 - Schema Administration and Publication

(1) The ADY61 profile describes how administrative areas must be set up and subdivided into manageable portions, and ways in which the operation of the Directory and of the administrative

areas are optimized through coordination of knowledge distribution, authentication and access control policies, distribution of naming contexts, etc. The use of quality requirements and resulting policies shall be the basis for the coordination procedures.

(2) The ADY62 profile describes how the initial phase of establishing a shadowing agreement shall be conducted for smooth introduction and utilization of the shadowing itself, and in addition, how the organizational management of such agreements shall be conducted, up to and including their dissolution.

(3) The ADY63 profile specifies how an administrative area shall administrate and publish its schema so that other administrative areas can be informed about the schema rules in use by the publishing area.

f. ADY7 - DOP Capabilities

The ADY7 class of profiles specifies the capabilities of a DSA for the using DOP facility to manage operational bindings. There are three functional profiles in this class:

- ADY71 - Shadowing Operational Binding
- ADY72 - Hierarchical Operational Binding
- ADY73 - Non-specific Hierarchical Operational Binding

(1) The ADY71 profile specifies how DOP is used by DSAs to establish, modify, and terminate shadow operational bindings in order to manage the standardized aspects of shadowing agreements.

(2) The ADY72 profile specifies how DOP is used by DSAs to establish, modify and terminate HOBs in order to manage the relationship and promulgate relevant information between two master DSAs. The DSAs hold naming contexts where one is immediately subordinate to the other and the superior DSA holds a subordinate reference to the subordinate DSA.

(3) The ADY73 profile specifies how DOP is used by DSAs to establish, modify and terminate Non-specific HOBs in order to manage the relationship and promulgate relevant information between two master DSAs. The DSAs hold naming contexts where one is immediately subordinate to the other and the superior DSA holds a non-specific subordinate reference to the subordinate DSA.

3. Directory Information Format and Representation Profiles

a. FDY1 - Schema

The FDY1 class of profiles specifies the Directory information that is common to a variety of applications. The Directory information covered includes both user information (placed in the Directory by, or on behalf of, users) and administrative and operational information (held and managed

by the Directory to meet various administrative and operational requirements). There are two functional profiles in this class:

- FDY11- Common Directory Use
- FDY12 - Directory System Schema

(1) The FDY11 profile covers user information to be stored within the Directory that is common to a variety of applications. FDY11 defines the minimum capabilities that a DUA and a DSA shall support in order to share a basic common view of the Directory user information. It does this by specifying a minimum set of object classes, attribute types, name forms, structure rules and matching rules to be supported.

(2) The FDY12 covers administrative and operational information a DSA shall hold to operate properly. It includes support of schema for the administrative and operational information model, schema for access control, and schema for collective attributes. FDY12 defines the minimum capabilities that a DUA and a DSA shall support in order to share a basic common view of the Directory administrative and operational information. It does this by specifying a minimum set of requirements concerning the specific tree structure for operational information and the operational content of the entries and subentries.

b. Application-Specific Directory Functional Profiles

(1) There are five applications that have functional profiles defined for Directory information and schema aspects that are required by the application:

- FDY2 - MHS Use of the Directory
- FDY3 - FTAM Use of the Directory
- FDY4 - TP Use of the Directory
- FDY5 - VT Use of the Directory
- FDY6 - EDI Use of the Directory

(2) Of these profiles, FDY2, MHS Use of the Directory, is applicable to components of the Allied Directory System. However, a complete FDY2 does not exist yet. In the future, FDY6, EDI Use of the Directory may be required.

(3) The FDY2 profile defines Directory user information concerning MHS that is needed in addition to the common information defined in FDY11. FDY2 defines the minimum capabilities that DSAs must have to support an MHS application's view of Directory information. It does this by specifying a minimum set of structure and naming elements for the DIT which a DSA must be capable of holding and accessing, and other minimum schema requirements.

4. Directory ISPs

Standard functional profiles are published in a type of document ISP. One or more functional profiles can be published in one ISP. As can be seen in Figure C-10, the directory Application Profiles are contained in one ISP that has a separate part corresponding to each functional profile. The generic directory Information Format and Representation Profiles are also contained in a multi-part ISP. However, each of the application-specific directory functional profiles is contained in a separate ISP.

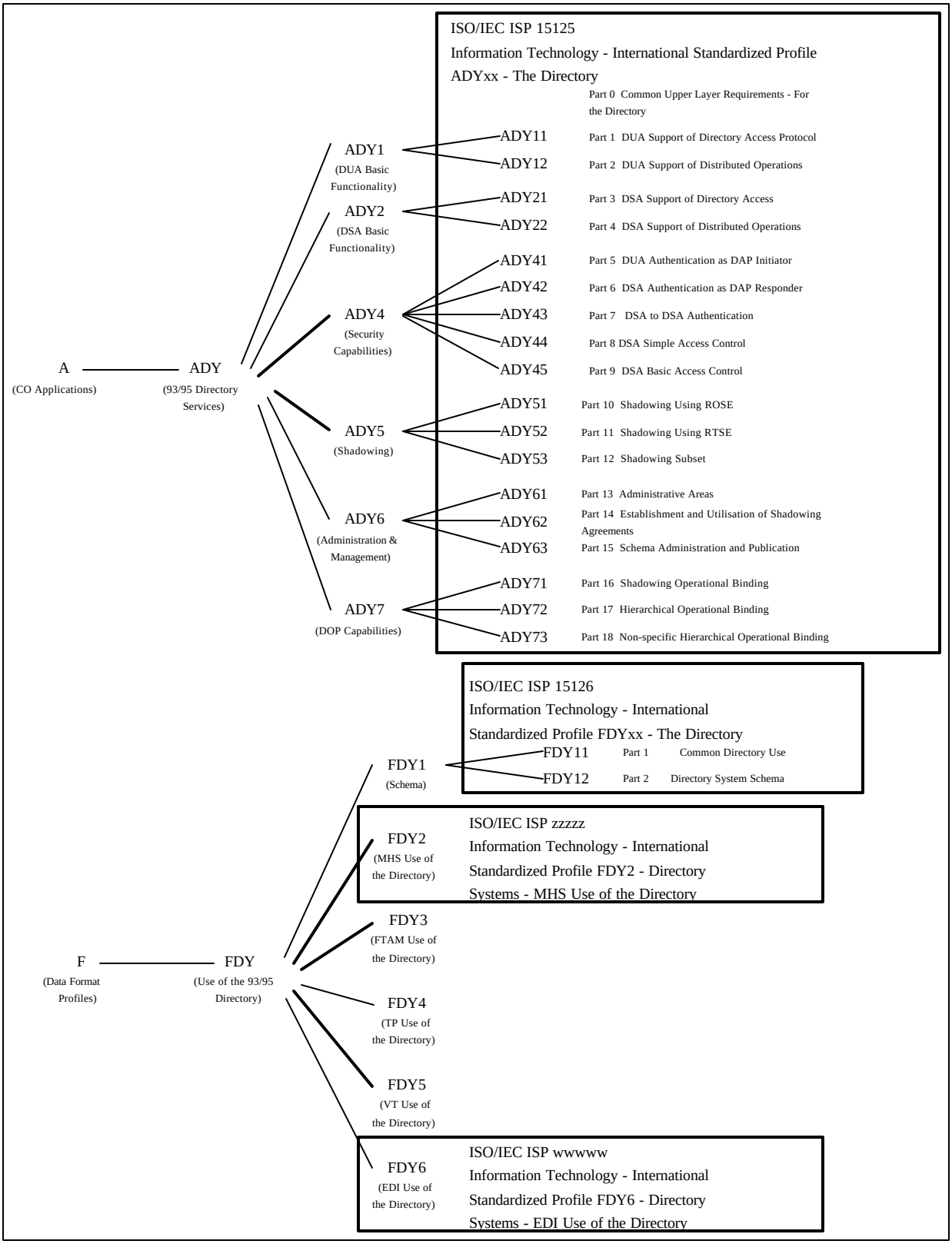

Figure C-10

Organization of Directory Functional Profiles Into International Standardized Profiles

ANNEX D

ALLIED DIRECTORY SYSTEM FUNCTIONAL PROFILES

TABLE OF CONTENTS

List of Tables

SECTION I

INTRODUCTION

1. General

a. This annex profiles the X.500 directory to satisfy the functionality required in the Allied Directory. In general, responses to requirements for implementations are made in a PICS. In a few cases where tables do not exist in the PICS, responses are made in an ISP. Where PICS and ISPs do not exist (for the 1997 edition of the Directory, for example) PICS responses should be made in this profile.

b. Annex D is divided into four sections. Section II specifies additions to the requirements of the Directory ISPs. The ACP 133 profiles are defined by showing the differences and additions to the cited ISP tables. That is, the tables shown are adapted extracts (including notes) from the ISP tables. Text in the ISPs should be consulted for additional guidance.

c. For a particular ISP, the global table of conformance may show a predicate. For example, in Table D-1, item 9, the ACP 133 requires that a DSA be able to be used as a repository for strong authentication information. A predicate of p_strong_rep is set. In subsequent tables, support of attributes in the ISP that are conditional on p_strong_rep is mandatory.

d. Where parameters are mandated and default values are permitted, implementations shall also support non-default values.

e. Section III specifies system schema requirements for ADUAs based on the FDY12 ISP, which does not include DUA requirements because of the large variety of DUAs.

f. Section IV includes protocol and schema requirements beyond those in the current ISPs and PICS. A column, "PICS Response", is included in the tables in this section. These tables include items from X.402, RFC 1274, ACP 133-specified schema items, and selected items from the 1997 Directory standards. The completed tables should be submitted with the applicable PICS.

SECTION II

ACP 133 ADDITIONS TO CURRENT ISPS AND PICS

2. Schema

a. Common Content

(1) DSAs and DUAs shall conform to ISO/IEC ISP 15126-1 (FDY11). The profile requirements for a single DSA for common directory use are given in Annex A and those for a DUA in Annex B of that document. The additional requirements in the tables in this paragraph shall also be met.

Column D represents the X.500 and X.400 standard requirement; column P represents the requirement of the ISP; column ACP represents the requirement of this profile. If the D & P requirements are the same, the columns are combined.

(2) Table D-1 is an adaptation of the table in clause A.1.2 in FDY11.

Table D-1
Identification of the Implementation and/or System - Single DSA

Item	Question	D	P	ACP 133	Predicate
8	Can the DSA be configured as a first-level DSA	o	yes/ no	yes	p_firstlevel
9	Can the DSA be used as a repository for strong authentication information?	o	yes/ no	yes	p_strong_rep
12	Does the DSA support the Content Rule mechanism defined in ITU-T X.501 | ISO/IEC 9594-2, 12.7?	o	yes/ no	yes	
13	Does the DSA support the Structure Rule mechanism defined in ITU-T X.501 | ISO/IEC 9594-2, 12.6?	o	yes/ no	yes	
14	Does the DSA return Collective Attributes in respect to Read and Search operations?	o	yes/ no	yes	p_collective_Attr
15	Does the DSA fully support Collective Attributes in Search filter?	o	yes/ no	yes	p_collective_Attr
16	Does the DSA fully support Collective Attributes in Compare operations?	o	yes/ no	yes	p_collective_Attr
17	Does the DSA return Attribute Subtypes in respect to Read and Search operations?	o	yes/ no	yes	p_Attr_subtyping
18	Does the DSA fully support Attribute Subtypes in Search filter?	o	yes/ no	yes	p_Attr_subtyping
19	Does the DSA fully support Attribute Subtypes in Compare operations?	o	yes/ no	yes	p_Attr_subtyping

(3) Table D-2 is an adaptation of the table in clause B.1.2 in FDY11.

Table D-2
Identification of the Implementation and/or System - DUA

Item	Question	D	P	ACP 133	Predicate
7	Does the DUA support strongAuthentication?	o	yes/no	yes	p_strong
10	Does the DUA support Attribute Subtypes in respect to Read and Search operations?	o	yes/no	yes	p_Attr_subtyping

(4) Table D-3 shows the collective attribute types, defined in X.520, that shall be supported. This is an adaptation of Table A.6.4.2.3 in FDY11.

Table D-3
X.520 Collective Attribute Types

Ref. no.	Collective Attribute Type	D & P	ACP 133	Notes
1	collectiveLocalityName	o	m	
2	collectiveStateOrProvinceName	o	m	
3	collectiveStreetAddress	o	m	
4	collectiveOrganizationName	o	m	
5	collectiveOrganizationalUnitName	o	m	
6	collectivePostalAddress	o	m	
7	collectivePostalCode	o	m	
8	collectivePostOfficeBox	o	m	
9	collectivePhysicalDeliveryOfficeName	o	m	
10	collectiveTelephoneNumber	o	m	
11	collectiveTelexNumber	o	m	
12	collectiveTeletexTerminalIdentifier	o	m	

Table D-3
X.520 Collective Attribute Types

Ref. no.	Collective Attribute Type	D & P	ACP 133	Notes
13	collectiveFacsimileTelephoneNumber	o	m	
14	collectiveInternationalISDNNumber	o	m	

(5) Table D-4 is an adaptation of the table in clause A.6.5.2 in FDY11.

Table D-4
Standard Matching Rules

Ref. no.	Matching Rule	D	P	ACP 133	Notes
2	caseIgnoreOrderingMatch	o	o	m	
17	octetStringOrderingMatch	o	o	m	
25	uTCTimeOrderingMatch	o	o	m	
27	generalizedTimeOrderingMatch	o	o	m	
35	accessPointMatch	o	o	m	
36	masterAndShadowAccessPointMatch	o	o	m	
37	supplierAndConsumerMatch	o	o	m	
38	supplierOrConsumerInformationMatch	o	o	m	

b. Allied Directory System Schema

(1) DSAs and DUAs shall conform to ISO/IEC ISP 15126-2 (FDY12). The profile requirements for a single DSA are given in Annex A of that document. The additional requirements in the tables in this paragraph shall also be met. Column D represents the X.500 standard requirement; column P represents the requirement of the ISP; column ACP represents the requirement of this profile. If the D & P requirements are the same, the columns are combined.

(2) Table D-5 is an adaptation of the table in clause A.1.2 in FDY12.

Table D-5
Identification of the Implementation and/or System - Single DSA

Item	Question	D	P	ACP 133	Predicate
7	Does the DSA support subschema administration?	o	yes/ no	yes	p_subschema
8	Does the DSA support collective attributes?	o	yes/ no	yes	p_collectiveAttr
9	Does the DSA support Simplified Access Control?	o	yes/ no	yes	p_AccessControl
10	Does the DSA support Basic Access Control?	o	yes/ no	yes	p_AccessControl
11	Does the DSA support Directory information shadow service specified in ITU-T X.525 | ISO/IEC 9594?	o	yes/ no	yes	p_shadow

(3) Table D-6 is an adaptation of the table in clause A.6.4.2.1 in FDY12.

Table D-6
Standard Operational Attribute Types - DSA Support

Ref. no.	Attribute Type	D &P	ACP 133	Notes
15	structuralObjectClass	o	m	
16	governingStructureRule	o	m	
22	myAccessPoint	o	m	
25	nonSpecificKnowledge	o	m	

3. DUAs

a. DUAs shall conform to ISO/IEC ISP 15125-1 (ADY11). The additional requirements for ACP 133 are summarized in the paragraphs below. The clauses cited refer to ADY11. Column D represents the X.500 standard requirement, column P represents the requirements of the ISP, and the Inter, Inter/Mod, and Adm columns represent the interrogation, interrogation/modification and administrative DUAs described in paragraph 219 of this ACP.

b. Table D-7 contains the differences from clause A.4.3.2.1, Operations.

Table D-7
Operations

Item	Operation	D	P	ACP 133			Predicate	Note
				Inter	Inter/ Mod	Adm		
3	Read	o	o	m	m	m	Read	
4	Compare	o	o	m	m	m	Compare	
5	Abandon	cn	c3	m	m	m	Abandon	Note 1
6	List	o	o	m	m	m	List	
7	Search	o	o	m	m	m	Search	
8	AddEntry	o	o	o	m	m	AddEntry	
9	RemoveEntry	o	o	o	m	m	RemoveEntry	
10	ModifyEntry	o	o	o	m	m	ModifyEntry	
11	ModifyDN	o	o	o	m	m	ModifyDN	

c3: If [Async-DUA], then support of this feature is o.

Note 1: The Abandon operation can only be supported if the asynchronous mode (ROSE class 2) of operation is supported for the DUA.

c. Table D-8 contains the differences from clause A.4.3.2.2, Extensions. This table defines a number of extensions which are available in the 1993 edition of the Directory. The supplier of the implementation shall indicate for which extensions conformance is claimed.

Table D-8
Extensions

Item No.	Operation	D	P	ACP 133			Predicate	Note
				Inter	Inter/Mod	Adm		
1	subentries	o	o	o	o	m		
4	extraAttributes	o	o	o	o	m		
5	modifyRightsRequest	o	o	o	o	m	modrightsreq	
10	useAliasOnUpdate	o	o	o	m	m		
11	newSuperior	o	o	o	o	m	newsuperior	

d. Table D-9 contains the differences from clause A.4.3.3.15, Service Controls.

Table D-9
Service Controls

Item No.	Operation	D	P	ACP 133			Predicate	Note
				Inter	Inter/Mod	Adm		
1	options	o	o	m	m	m		
2	priority	o	o	m	m	m		

e. Table D-10 contains the differences from clause A.4.3.3.16, Entry Information Selection.

Table D-10
Entry Information Selection

Item No.	Operation	D	P	ACP 133			Predicate	Note
				Inter	Inter/Mod	Adm		
3	extraAttributes	o	o	o	o	m		

f. DUAs shall conform to ISO/IEC ISP 15125-2 (ADY12). There are no additional requirements for ACP 133.

g. DUAs shall conform to ISO/IEC ISP 15125-5 (ADY41). The additional requirements for ACP 133 are summarized in the paragraphs below. The clauses cited refer to ADY41. Column D represents the X.500 standard requirement, column P represents the requirements of the ISP, and the Inter, Inter/Mod, and Adm columns represent the types of DUAs described in paragraph 219 of this ACP.

h. Table D-11 is an adaptation of the table in clause A.4.2.1 in ADY41.

Table D-11
General Capabilities

Item No.	Operation	D	P	ACP 133			Predicate Name	Note
				Inter	Inter/ Mod	Adm		
5	Does the DUA support signed DAP operations and results?	o	o	o	o	m	*digitalSig	

i. Table D-12 is an adaptation of the table in clause A.4.2.2 in ADY41.

Table D-12
Supported Security Levels

Item No.	Operation	D	P	ACP 133			Reference	Note
				Inter	Inter/ Mod	Adm		
3	strong	cn	cl	m	m	m	*strongAuth	

cl: If [digitalSig], then support of this feature is m else o.

j. Table D-13 is an adaptation of the table in clause A.4.3.1.1 in ADY41.

Table D-13
Directory Bind Arguments

Item No.	Operation	D	P	ACP 133			Reference	Note
				Inter	Inter/ Mod	Adm		
1.2.1	certification-path	c:o	c:o.1	m	m	m		
1.2.3	name	c:o	c:o.1	o	o	o		Note 1

o.1 At least one or both of the certification-path and name must always be present, and if both, then they must “agree”, i.e., indicate the same name.

Note 1: The name should be absent; the subject name within the user certificate contains the same information. Access control decisions should be based on authenticated information in the certificate, not on the unauthenticated name in the StrongCredentials.

k. Table D-14 contains the differences from ADY41, clause A.4.3.3.22, Security Parameters. Requirements for use of the 1997 enhancements to security parameters for ACP 133 DUAs are specified in Annex D, Section IV, paragraph 7.

Table D-14
Security Parameters

Item No.	Operation	D	P	ACP 133			Predicate	Note
				Inter	Inter/ Mod	Adm		
1	certification-path	m	m	c1	c1	m		Note 1
5	target	o	m	o	o	o		Note 2

c1: If [digitalSig], then support of this feature is m else o.

Note 1: As specified for the Certificate Management Infrastructure (CMI).

Note 2: The policy shall define minimum levels for the target protection levels.

l. Table D-15 is an adaptation of the table in clause B.3 in ADY41.

Table D-15
General Security

Item No.	Operation	D	P	ACP 133			Predicate Name	Notes
				Inter	Inter/ Mod	Adm		
2	Does the DUA support certificates?	o	o	m	m	m		
3	Does the DUA support Certificate Revocation List?	o	o	m	m	m		
4	Does the DUA support Authority Revocation List?	o	o	m	m	m	*arl	
5	Does the DUA support the ASN.1 Distinguished Encoding Rules (DER)?	o	o	m	m	m		Note 1

Note 1: DUAs shall conform to the encoding rules as specified in [ISO/IEC 9594-8: 1993 | ITU-T Rec. X.509 (1993)] Clause 9.

m. Table D-16 is an adaptation of the table in clause B.5 in ADY41.

Table D-16
Strong Authentication

Item No.	Operation	D	P	ACP 133			Predicate Name	Note
				Inter	Inter/ Mod	Adm		
1	Does the DUA support Strong Authentication on Bind Request?	o	o	m	m	m		Note 3
1.2	Two-way	c:o	c:o	m	m	m		
2	Does the DUA support Strong Authentication on Bind Result?	o	o	m	m	m		Note 3
3	Does the DUA support strong authentication in the initiator role?	o	o	m	m	m	*strong Auth	Note 3
4	Does the DUA support strong authentication in the responder role?	o	o	m	m	m	*strong Auth	Note 3
5	Does the DUA support the generation of certification path for strong authentication?	o	o	m	m	m	certPath	

Note 3: A positive response implies support for strong authentication
(See A.4.2.2/3 in Annex A of ISP 15125-5)

n. Table D-17 is an adaptation of the table in clause B.6 in ADY41. Requirements for use of the 1997 signed operation enhancements for DAP in ACP 133 DUAs are specified in Section IV paragraph 7.

Table D-17
Signed Operations

Item No.	Operation	D	P	ACP 133			Predicate Name	Note
				Inter	Inter/ Mod	Adm		
5	Does the DUA support Signed Add Entry?	o	o	o	o	m	*signAdd	Note 5
6	Does the DUA support Signed Remove?	o	o	o	o	m	*signRemove	Note 5
7	Does the DUA support Signed Modify Entry?	o	o	o	o	m	*signModify	Note 5
8	Does the DUA support Signed ModifyDN?	o	o	o	o	m	*signModDN	Note 5

Note 5: A positive response implies support for Signed DAP operations
(See A.4.2.1/5 in Annex A of ISP 15125-5)

4. DSAs

a. DAP

(1) DSAs shall conform to ISO/IEC ISP 15125-3 (ADY21). The additional requirements for ACP 133 are summarized in the paragraphs below. The clauses cited refer to ADY21. Column D represents the X.500 standard requirement, column P represents the requirements of the ISP, and the ACP column represents the requirements of this ACP.

(2) Table D-18 contains the differences from clause A.4.2.1,General Capabilities.

Table D-18
General Capabilities

Item No.	Operation	D	P	ACP	Predicate	Note
8	Is the DSA capable of supporting collective attributes?	o	o	m		
9	Is the DSA capable of supporting hierarchical attributes (Subtypes)?	o	o	m		

(3) Table D-19 contains the differences from clause A.4.3.2.1, Operations.

Table D-19
Operations

Item No.	Operation	D	P	ACP	Predicate	Note
5	Abandon	cn	c3	m	*Abandon	

c3: If [Async-DSA],then support of this feature is o.

(4) DSAs shall conform to ISO/IEC ISP 15125-6 (ADY42). The additional requirements for ACP 133 are summarized in the paragraphs below. The clauses cited refer to ADY42. Column D represents the X.500 standard requirement, column P represents the requirements of the ISP, and the ACP column represents the requirements of this ACP.

(5) Table D-20 is an adaptation of the table in clause A.4.2.1 in ADY42.

Table D-20
General Capabilities

Item No.	Operation	D	P	ACP	Reference	Notes
5	Does the DSA support signed DAP operations and results?	o	o	m	*digitalSig	

(6) Table D-21 is an adaptation of the table in clause A.4.2.2 in ADY42.

Table D-21
Supported Security Levels

Item No.	Operation	D	P	ACP	Reference	Notes
3	strong	o.n	c1	m	*strongAuth	

c1: If [digitalSig], then support of this feature is m else o.

(7) Table D-22 is an adaptation of the table in clause B.3 in ADY42.

Table D-22
General Security

Item No.	Operation	D	P	ACP	Reference	Notes
2	Does the DSA support Certificates?	o	o	m		
3	Does the DSA support Certificate Revocation List?	o	o	m		
4	Does the DSA support Authority Revocation List?	o	o	m	*arl	
5	Does the DSA support the ASN.1 Distinguished Encoding Rules (DER)?	o	o	m		

(8) Table D-23 is an adaptation of the table in clause B.5 in ADY42.

Table D-23
Strong Authentication

Item No.	Operation	D	P	ACP	Reference	Notes
1	Does the DSA support Strong Authentication on Bind Request?	o	o	m		
1.2	Two-way	c:o	c:o	m	*arl	
2	Does the DSA support Strong Authentication on Bind Result?	o	o	m		
3	Does the DSA support strong authentication in the initiator role?	o	o	m	*strongAuth	

Table D-23
Strong Authentication

Item No.	Operation	D	P	ACP	Reference	Notes
4	Does the DSA support strong authentication in the responder role?	o	o	m	*strongAuth	
5	Does the DSA support the generation of certification path for strong authentication?	o	o	m		

(9) Table D-24 is an adaptation of the table in clause B.6 in ADY42. Requirements for use of the 1997 signed operation enhancements for DAP in ACP 133 DSAs are specified in Section IV, paragraph 8a.

Table D-24
Signed Operations

Item No.	Operation	D	P	ACP	Reference	Notes
5	Does the DSA support Signed Add Entry?	o	o	m	*signAdd	
6	Does the DSA support Signed Remove Entry?	o	o	m	*signRemove	
7	Does the DSA support Signed Modify Entry?	o	o	m	*signModify	
8	Does the DSA support Signed ModifyDN?	o	o	m	*signModDN	

(10) DSAs shall conform to ISO/IEC ISP 15125-9 (ADY45). The additional requirements for ACP 133 are summarized in the paragraphs below. The clauses cited refer to ADY45. Column D represents the X.500 standards requirement, column P represents the requirements of the ISP, and the ACP column represents the requirements of this ACP.

(11) Table D-25 shows the differences from clause A.4.2.3 of ADY45.

Table D-25
Supported Access Control Schemes

Item No.	Question	D	P	ACP	Predicate	Note
2	Basic Access Control	o	o.1	m	*BAC-DSA	

(12) Table D-26 shows the differences from clause B.3 of ADY45.

Table D-26
Access Support

Item No.	Question	D	P	ACP	Predicate	Note
7	Does the DSA support Import for entry access?	o	o	m	*importEntry	
8	Does the DSA support Export for entry access?	o	o	m	*exportEntry	
9	Does the DSA support ReturnDN for entry access?	o	o	m	*returnDNEntry	

b. DSP

(1) DSAs shall conform to ISO/IEC ISP 15125-4 (ADY22). The additional requirements for ACP 133 are summarized in the paragraphs below. The clauses cited refer to ADY22. Column D represents the X.500 standard requirement, column P represents the requirements of the ISP, and the ACP column represents the requirements of this ACP.

(2) Table D-27 shows the differences from clause A.3.1 of ADY22.

Table D-27
DSA implementation and/or system

Item No.	Question	D	P	ACP	Predicate Name or note
6	Are Cross References supported?	o	o	m	p_cross_references
9	Are Master References supported	-	o	m	p_master_reference

Table D-27
DSA implementation and/or system

Item No.	Question	D	P	ACP	Predicate Name or note
12	Are Hierarchical operational bindings supported?	-	o	m	p_hob
18	Does the DSA support being a non-first-level DSA?	-	o	m	p_non_first_level_dsa
19	Does the DSA support the invoker role?	-	o	m	p_invoker
23	Does the DSA support strong credentials in the DSA Bind?	o	o	m	p_strong Note 2
24	Does the DSA support signed chained operations?	o	o	m	p_signed_chained Note 2
26	Does the DSA support authentication level? (see [ISO/IEC 9594-4: 1993 | ITU-T Rec. X.518 (1993)] clause 10.3 m)	o	o	m	p_auth_level
28	Does the DSA support excludeShadows (see [ISO/IEC 9594-4: 1993 | ITU-T Rec. X.518 (1993)] clause 10.3 q)	o	o	m	p_excludeShadows
31	Does the DSA support creation of a request for cross-references (see [ISO/IEC 9594-4: 1993 | ITU-T Rec. X.518 (1993)] clause 10.3 f)	o	o	m	p_obtain_xr

Table D-27
DSA implementation and/or system

Item No.	Question	D	P	ACP	Predicate Name or note
32	Does the DSA support the supply of cross-references on request (see [ISO/IEC 9594-4: 1993 | ITU-T Rec. X.518 (1993)] clause 10.4 b)	o	o	m	p_supply_xr
33	Does the DSA support the request to return the operation to the DUA (see [ISO/IEC 9594-4: 1993 | ITU-T Rec. X.518 (1993)] clause 10.10 i)	o	o	m	p_return_to_dua

Note 2: Security levels are profiled in ADY43. They are represented in this PRL by the predicates p_simple_protected (A.3.1.22), p_strong (A.3.1.23), and p_signed_chained (A.3.1.24).

(3) DSAs shall conform to ISO/IEC ISP 15125-7 (ADY43). This ISP defines strong authentication for DSP, DISP, and DOP. The additional requirements for ACP 133 are summarized in the paragraphs below. The clauses cited refer to ADY43. Column D represents the X.500 standard requirement, column P represents the requirements of the ISP, and the ACP column represents the requirements of this ACP. Requirements for use of the 1997 signed operation enhancements for DSP and DISP in ACP 133 are specified in Section IV, paragraphs 8b and 8c.

(4) Table D-28 specifies the differences from clause A.3.1, Global statement of conformance - DSP.

Table D-28
Global Statement of Conformance - DSP

Item No.	Question	D	P	ACP	Predicate Name or note
1	Does the DSA support DSA Binds in the initiator role?	o	o	m	p_dsa_bind_ini
2	Does the DSA support DSA Binds in the responder role?	o	o	m	p_dsa_bind_resp

Table D-28
Global Statement of Conformance - DSP

Item No.	Question	D	P	ACP	Predicate Name or note
5	Does the DSA support DSA Binds using strong credentials in the initiator role?	o	o	m	p_dsa_strong_ini
6	Does the DSA support DSA Binds using strong credentials in the responder role?	o	o	m	p_dsa_strong_resp
7	Does the DSA support the invoker role in DSP operations?	o	o	m	p_dsp_invoker
8	Does the DSA support signed DSP operations in both invoker and performer roles	o	o	m	p_signed_dsp
10	Does the DSA support authentication level in ChainingArguments	o	o	m	p_dsp_auth_level

(5) Table D-29 specifies the differences from clause A.3.4, Global statement of conformance - all supported protocols.

Table D-29
Global Statement of Conformance - DSP, DOP, DISP

Item No.	Question	D	P	ACP	Predicate Name or note
2	Does the DSA support two-way authentication in strong binds?	o	o	m	p_2way_strong
3	Does the DSA support two-way authentication in signed operations?	o	o	m	p_2way_signed
8	Does the DSA support Certificate Revocation Lists Version 2?	o	o	m	p_crl_v2

(6) DSAs shall conform to ISO/IEC ISP 15125-13 (ADY61). Table D-30 specifies the differences from clause A.3.1, General Capabilities.

Table D-30
General Capabilities

Item No.	Question	D	P	ACP	Predicate Name or note
2	Does the DSA support subschema administrative areas?	o	o	m	subschema
4	Does the DSA support access control inner administrative areas?	cl	cl	m	ACinner
5	Does the DSA support collective-attribute specific administrative areas?	o	o	m	ColAtSpec
6	Does the DSA support collective-attribute inner administrative areas?	o	o	m	ColAtInner
7	Does the DSA support multipurpose subentries?	o	o	m	MulPurSE

c.1: If BAC supported m then i.

(7) DSAs shall conform to ISO/IEC ISP 15125-9 (ADY45). The additional requirements for ACP 133 are summarized in the paragraphs below. The clauses cited refer to ADY45. Column D represents the X.500 standards requirement, column P represents the requirements of the ISP, and the ACP column represents the requirements of this ACP.

(8) Table D-31 shows the differences from clause A.5.2.3 of ADY45.

Table D-31
Supported Access Control Schemes

Item No.	Question	D	P	ACP	Predicate	Note
2	Basic Access Control	o	o.1	m	*BAC-DSA	

(9) Table D-32 shows the differences from clause B.3 of ADY45.

Table D-32
Access Support

Item No.	Question	D	P	ACP	Predicate	Note
7	Does the DSA support Import for entry access?	o	o	m	*importEntry	
8	Does the DSA support Export for entry access?	o	o	m	*exportEntry	
9	Does the DSA support ReturnDN for entry access?	o	o	m	*returnDNEntry	

c. DISP

(1) DSAs shall conform to ISO/IEC ISP 15125-7 (ADY43). This ISP defines strong authentication for DSP, DISP, and DOP. The additional requirements for ACP 133 are summarized in the paragraphs below. The clauses cited refer to ADY43. Column D represents the X.500 standard requirement, column P represents the requirements of the ISP, and the ACP column represents the requirements of this ACP.

(2) Table D-33 specifies the differences from clause A.3.3, Global statement of conformance - DISP.

Table D-33
Global Statement of Conformance - DISP

Item No.	Question	D	P	ACP	Predicate Name or note
1	Does the DSA support the application-context: shadowSupplierInitiatedAC?	o	o	m	p_disp_sup_ini
2	Does the DSA support the application-context: reliableshadowSupplierInitiatedAC?	o	o	o	p_disp_rel_sup_ini Note 1
3	Does the DSA support the application-context: shadowConsumerInitiatedAC?	o	o	m	p_disp_cons_ini
4	Does the DSA support the application-context: reliableshadowConsumerInitiatedAC?	o	o	o	p_disp_rel_cons_ini Note 1

Table D-33
Global Statement of Conformance - DISP

Item No.	Question	D	P	ACP	Predicate Name or note
5	Does the DSA support DISP Binds in the initiator role?	o	o	m	p_disp_bind
6	Does the DSA support DISP Binds in the responder role?	o	o	m	p_disp_simp_unprot_resp
9	Does the DSA support DISP Binds at least using strong credentials in the initiator role?	o	o	m	p_disp_strong_ini
10	Does the DSA support DISP Binds at least using strong credentials in the responder role?	o	o	m	p_disp_strong_resp
11	Does the DSA support signed DISP operations in both invoker and performer roles?	o	o	m	p_signed_disp

Note 1: The use of the RTSE-inclusive application contexts may be mandated by the tactical community.

(3) Table D-29 also applies.

(4) DSAs shall conform to ISO/IEC ISP 15125-10 (ADY51). The additional requirements for ACP 133 are summarized in the paragraphs below. The clauses cited refer to ADY51. Column D represents the X.500 standard requirement, column P represents the requirements of the ISP, and the ACP column represents the requirements of this ACP.

(5) Table D-34 specifies the differences from clause A.3 of ADY51.

Table D-34
Global Statement of Conformance

Ref.No.	Question	D	P	ACP	Predicate	Notes
5	Is security level "strong" for peer entity authentication supported?	o.1	o	m	Strong-auth	
6	Are signed DISP operations supported?	o	o	m	Signed-ops	

Table D-34
Global Statement of Conformance

Ref.No.	Question	D	P	ACP	Predicate	Notes
7	Is the incremental update strategy supported?	o	o	m	Inc-updates	
8	Is secondary shadowing supported?	o	o	m		

o.1: At least one of the security levels for peer entity authentication shall be supported.

(6) DSAs shall conform to ISO/IEC ISP 15125-12 (ADY53). The additional requirements for ACP 133 are summarized in the paragraphs below. The clauses cited refer to ADY53. Column D represents the X.500 standard requirement, column P represents the requirements of the ISP, and the ACP column represents the requirements of this ACP.

(7) Table D-35 specifies the differences from clause A.3.1 of ADY53.

Table D-35
DSA Implementation

Ref. No.	Question	Response	ACP
1	Shadow Supplier Role Supported	yes/no	yes
2	Shadow Consumer Role Supported	yes/no	yes
3	Empty Context Prefix in Replicated Area Supported	yes/no	yes

The following predicates are defined: p_sup = A.3.1/1, p_con = A.3.1/2, and p_ecp = A.3.1/3

d. DOP

(1) DSAs shall conform to ISO/IEC ISP 15125-7 (ADY43). This ISP defines strong authentication for DSP, DISP, and DOP. The additional requirements for ACP 133 are summarized in the paragraphs below. The clauses cited refer to ADY43. Column D represents the X.500 standard requirement, column P represents the requirements of the ISP, and the ACP column represents the requirements of this ACP.

(2) Table D-36 specifies the differences from clause A.3.2, Global statement of conformance - DOP.

Table D-36
Global Statement of Conformance - DOP

Item No.	Question	D	P	ACP	Predicate Name or note
1	Does the DSA support Operational Binding type: shadowOperationalBindingID	o	o	m	p_sob
2	Does the DSA support Operational Binding type: SpecificHierarchicalBindingID	o	o	m	p_shob
4	Does the DSA support DOP Binds in the initiator role?	o	o	m	p_dop_bind_ini
5	Does the DSA support DOP Binds in the responder role?	o	o	m	p_dop_bind_resp
8	Does the DSA support DOP Binds using strong credentials in the initiator role?	o	o	m	p_dop_strong_ini
9	Does the DSA support DOP Binds using strong credentials in the responder role?	o	o	m	p_dop_strong_resp

(3) Table D-29 also applies.

(4) DSAs shall conform to ISO/IEC ISP 15125-16 (ADY71). The ACP requires support of both the shadowSupplierInitiatedAC and the ShadowConsumerInitiatedAC.

(5) DSAs shall conform to ISO/IEC ISP 15125-17 (ADY72). The additional requirements for ACP 133 are summarized in the paragraphs below. The clauses cited refer to ADY72. Column D represents the X.500 standard requirement, column P represents the requirements of the ISP, and the ACP column represents the requirements of this ACP.

(6) Table D-37 specifies the differences from clause 6 of ADY72.

Table D-37
Summary of Support

Ref. No.	Question	P	ACP 133
10	Support of transfer of administrative point and subentry information by ROLE A DSAs: Subschema information	o	m
11	Support of transfer of administrative point and subentry information by ROLE A DSAs: Collective attribute information	o	m
18	Support of DOP binds using strong authentication	o	m

SECTION III

DUA EXTENSIONS

5. Administrative DUAs

a. Because of the variety of DUAs, FDY12 does not include any tables for DUAs. Table D-38 identifies support required for ACP 133 ADUAs, which are required to maintain operational attributes in the directory. Responses should be made in the PICS. Interrogation and Interrogation/Modification DUAs have no requirement to view or modify operational attributes.

Table D-38
Identification of the Implementation and/or System - Administrative DUA

Item	Question	D	ACP 133	Predicate
1	Does the DUA support subschema administration?	o	yes	p_subschema
2	Does the DUA support collective attributes?	o	yes	p_collectiveAttr
3	Does the DUA support Simplified Access Control?	o	yes	p_AccessControl
4	Does the DUA support BasicAccess Control?	o	yes	p_AccessControl
5	Does the DUA support Directory information shadow service specified in ITU-T X.525 | ISO/IEC 9594?	o	yes	p_shadow

b. Table D-39 shows the standard object classes that shall be supported by ADUAs.

Table D-39
Standard Operational Object Classes - Administrative DUAs

Item	Object Class	D	ACP 133	Notes
1	subentry	m	C4	
2	subschemaSubentry	o	C1	
3	collectiveAttributeSubentry	o	C2	
4	accessControlSubentry	o	C3	

Conditionals:

C1: if p_subschema then m else o.

C2: if p_collectiveAttr then m else o.

C3: if p_AccessControl then m else o.

C4: if p_subschema or p_collectiveAttr or p_AccessControl then m else o.

c. Table D-40 shows the attribute types, defined in X.500 (1993), that shall be supported by ADUAs.

Table D-40
Standard Operational Attribute Types - Administrative DUAs

Item	Attribute Type	D	ACP 133	Notes
1	createTimeStamp	m	m	
2	modifyTimeStamp	o	m	
3	creatorsName	o	m	
4	modifiersName	o	m	
5	administrativeRole	o	C4	
6	subtreeSpecification	o	m	
7	collectiveExclusions	o	C2	
8	dITStructureRules	o	C1	
9	dITContentRules	o	C1	

Table D-40
Standard Operational Attribute Types - Administrative DUAs

Item	Attribute Type	D	ACP 133	Notes
10	matchingRules	o	C1	
11	attributeTypes	o	C1	
12	objectClasses	o	C1	
13	nameForms	o	C1	
14	matchingRuleUse	o	C1	
15	structuralObjectClass	o	m	
16	governingStructureRule	o	m	
17	accessControlScheme	o	C3	
18	prescriptiveACI	o	C3	
19	entryACI	o	C3	
20	subentryACI	o	C3	
21	dseType	o	m	
22	myAccessPoint	o	m	
23	superiorKnowledge	o	m	
24	specificKnowledge	o	m	
25	nonSpecificKnowledge	o	m	
26	supplierKnowledge	o	C5	
27	consumerKnowledge	o	C5	
28	secondaryShadows	o	C5	

Conditionals:

C1: if p_subschema then m else o.

C2: if p_collectiveAttr then m else o.

C3: if p_AccessControl then m else o.

C4: if p_subschema or p_collectiveAttr or p_accessControl then m else o.

C5: if p_shadow then m else o.

SECTION IV

ACP 133 PROTOCOL AND SCHEMA EXTENSIONS

6. Common Content Extensions

a. Object Classes

(1) Table D-41 shows the object classes, defined in X.402, that shall be supported.

Table D-41
X.402 Object Classes

Item	Object Class	D	ACP 133	Notes	PICS Response
1	mhs-distribution-list	o	m		
2	mhs-message-store	o	m		
3	mhs-message-transfer-agent	o	m		
4	mhs-user	o	m		
5	mhs-user-agent	o	m		

(2) Table D-42 shows the object classes, defined in this ACP, that shall be supported.

Table D-42
ACP 133 Object Classes

Item	Object Class	ACP 133	Notes	PICS Response
1	aCPNetworkEdB	m		
2	aCPNetworkInstructionsEdB	m		
3	addressList	m		
4	aliasCommonName	m		
5	aliasOrganizationalUnit	m		
6	altSpellingACP127	m		
7	cadACP127	m		
8	distributionCodeDescription	m		

Table D-42
ACP 133 Object Classes

Item	Object Class	ACP 133	Notes	PICS Response
9	distributionCodesHandled	m		
10	dSSCSPLA	m		
11	messagingGateway	m		
12	mLA	m	Note 1	
13	mLAgent	m		
14	network	m	Note 1	
15	networkInstructions	m	Note 1	
16	orgACP127	m		
17	otherContactInformation	m		
18	plaACP127	m		
19	plaCollectiveACP127	m		
20	plaData	m		
21	plaUser	m		
22	releaseAuthorityPerson	m	Note 1	
23	releaseAuthorityPersonA	m		
24	routingIndicator	m		
25	securePkiUser	m		
26	secure-user	m	Note 1	
27	sigintPLA	m		
28	sIPLA	m		
29	spotPLA	m		
30	taskForceACP127	m		
31	tenantACP127	m		
32	ukms	m		

Note 1: These object classes may be removed in a later edition of this ACP.

(3) Table D-43 shows the object classes, defined in the 1997 edition of the Directory specifications, that shall be supported.

Table D-43
1997 Standard Object Classes

Item	Object Class	D	ACP	Notes	PICS Response
1	certificationAuthority-V2	o	m	Note 1	
2	cRLDistributionPoint	o	m		
3	userSecurityInformation	o	m		

Note 1: This object class may be removed in a later edition of this ACP.

(4) Table D-44 shows the object classes, defined in X.509(1997) DAM 1, that shall be supported.

Table D-44
X.509(1997) DAM 1 Standard Object Classes

Item	Object Class	D	ACP	Notes	PICS Response
1	pkiCA	o	m		
2	pkiUser	o	m		

b. Attribute Types

(1) Table D-45 shows the attribute types, defined in X.402, that shall be supported.

Table D-45
X.402 Attribute Types

Item	Attribute Type	D	ACP 133	Notes	PICS Response
1	mhs-acceptable-eits	o	m		
2	mhs-deliverable-classes	o	m		

Table D-45
X.402 Attribute Types

Item	Attribute Type	D	ACP 133	Notes	PICS Response
3	mhs-deliverable-content-types	o	m		
4	mhs-dl-archive-service	o	m		
5	mhs-dl-members	o	m		
6	mhs-dl-policy	o	m		
7	mhs-dl-related-lists	o	m		
8	mhs-dl-submit-permissions	o	m		
9	mhs-dl-subscription-service	o	m		
10	mhs-exclusively-acceptable-eits	o	m		
11	mhs-maximum-content-length	o	m		
12	mhs-message-store-dn	o	m		
13	mhs-or-addresses	o	m		
14	mhs-or-addresses-with-capabilities	o	m		
15	mhs-supported-attributes	o	m		
16	mhs-supported-automatic-actions	o	m		
17	mhs-supported-content-types	o	m		
18	mhs-supported-matching-rules	o	m		
19	mhs-unacceptable-eits	o	m		

(2) Table D-46 shows the attribute types, defined in this ACP, that shall be supported.

Table D-46
ACP 133 Attribute Types

Item	Attribute Type	ACP133	Notes	PICS Response
1	accessCodes	m		
2	accessSchema	m	Note 1	
3	accountingCode	m		
4	aCPLegacyFormat	m		
5	aCPMobileTelephoneNumber	m		
6	aCPNetwAccessSchemaEdB	m		
7	aCPNetworkSchemaEdB	m		
8	aCPPagerTelephoneNumber	m		
9	aCPPreferredDelivery	m		
10	aCPTelephoneFacsimileNumber	m		
11	actionAddressees	m		
12	additionalAddressees	m		
13	additionalSecondPartyAddressees	m		
14	adminConversion	m		
15	administrator	m		
16	aigsExpanded	m		
17	aLExemptedAddressProcessor	m		
18	aliasPointer	m		
19	alid	m		
20	allowableOriginators	m		
21	aLReceiptPolicy	m		

Table D-46
ACP 133 Attribute Types

Item	Attribute Type	ACP133	Notes	PICS Response
22	alternateRecipient	m		
23	alType	m		
24	aprUKMs	m		
25	associatedAL	m		
26	associatedOrganization	m		
27	associatedPLA	m		
28	augUKMs	m		
29	cognizantAuthority	m		
30	community	m		
31	copyMember	m		
32	decUKMs	m		
33	deployed	m		
34	distributionCodeAction	m		
35	distributionCodeInfo	m		
36	dualRoute	m		
37	effectiveDate	m		
38	entryClassification	m		
39	expirationDate	m		
40	febUKMs	m		
41	garrison	m		
42	gatewayType	m		

Table D-46
ACP 133 Attribute Types

Item	Attribute Type	ACP133	Notes	PICS Response
43	ghpType	m		
44	guard	m		
45	hostOrgACP127	m		
46	infoAddressees	m		
47	janUKMs	m		
48	julUKMs	m		
49	junUKMs	m		
50	lastRecapDate	m		
51	listPointer	m		
52	lmf	m		
53	longTitle	m		
54	mailDomains	m		
55	marUKMs	m		
56	mayUKMs	m		
57	militaryFacsimileNumber	m		
58	militaryTelephoneNumber	m		
59	nameClassification	m		
60	nationality	m		
61	networkDN	m		
62	networkSchema	m	Note 1	
63	novUKMs	m		

Table D-46
ACP 133 Attribute Types

Item	Attribute Type	ACP133	Notes	PICS Response
64	octUKMs	m		
65	onSupported	m		
66	operationName	m		
67	plaAddressees	m		
68	plaNameACP127	m		
69	plaReplace	m		
70	positionNumber	m		
71	primarySpellingACP127	m		
72	proprietaryMailboxes	m		
73	publish	m		
74	rank	m		
75	recapDueDate	m		
76	releaseAuthorityName	m		
77	remarks	m		
78	rI	m		
79	rIClassification	m		
80	rIInfo	m		
81	secondPartyAddressees	m		
82	section	m		
83	secureFacsimileNumber	m		
84	secureTelephoneNumber	m		

Table D-46
ACP 133 Attribute Types

Item	Attribute Type	ACP133	Notes	PICS Response
85	sepUKMs	m		
86	serviceNumber	m		
87	serviceOrAgency	m		
88	sHD	m		
89	shortTitle	m		
90	sigad	m		
91	spot	m		
92	tARE	m		
93	tCC	m		
94	tCCG	m		
95	transferStation	m		
96	tRC	m		
97	usdConversion	m		

Note 1: These attribute types may be removed in a later edition of this ACP.

(3) Table D-47 shows the attribute types, defined in RFC 1274, that shall be supported.

Table D-47
RFC 1274 Attribute Types

Item	Attribute Type	ACP 133	Notes	PICS Response
1	host	m		
2	rfc822Mailbox	m	also known as mail	
3	roomNumber	m		

(4) Table D-48 shows the attribute types, defined in the 1997 edition of the Directory specifications, that shall be supported.

Table D-48
1997 Standard Attribute Types

Item	Attribute Type	D	ACP 133	Notes	PICS Response
1	attributeCertificate	o	m		
2	clearance	o	m	used in certificate extension	
3	deltaRevocationList	o	m		
4	supportedAlgorithms	o	m		

(5) Table D-49 shows the collective attribute types, defined in this ACP, that shall be supported.

Table D-49
ACP 133 Collective Attribute Types

Item	Collective Attribute Type	D & P	ACP 133	Notes	PICS Response
1	collective-mhs-or-addresses	-	m		
2	collectiveMilitaryFacsimileNumber	-	m		
3	collectiveMilitaryTelephoneNumber	-	m		
4	collectiveNationality	-	m		
5	collectiveSecureFacsimileNumber	-	m		
6	collectiveSecureTelephoneNumber	-	m		

c. Name Forms

(1) Table D-50 shows the name forms, defined in this ACP, that shall be supported.

Table D-50
ACP 133 Name Forms

Item	Name Form	D & P	ACP 133	Notes	PICS Response
1	aCPNetworkEdBNameForm	-	m		
2	aCPNetworkInstrEdBNameForm	-	m		
3	addressListNameForm	-	m		
4	aENameForm	-	m		
5	aliasCNNameForm	-	m		
6	aliasOUNameForm	-	m		
7	alternateSpellingPLANameForm	-	m		
8	cadPLANameForm	-	m		
9	distributionCodeDescriptionNameForm	-	m		
10	dSSCSPLANameForm	-	m		
11	messagingGatewayNameForm	-	m		
12	mhs-dLNameForm	-	m		
13	mLANameForm	-	m	Note 1	
14	mLAgentNameForm		m		
15	mSNameForm	-	m		
16	mTANameForm	-	m		
17	mUANameForm	-	m		
18	networkNameForm	-	m	Note 1	
19	networkInstructionsNameForm	-	m	Note 1	
20	organizationalPLANameForm	-	m		
21	organizationNameForm	-	m		
22	orgRNameForm	-	m		
23	orgUNameForm	-	m		
24	plaCollectiveNameForm	-	m		
25	qualifiedOrgPersonNameForm	-	m		
26	releaseAuthorityPersonNameForm	-	m	Note 1	
27	releaseAuthorityPersonANameForm		m		

Table D-50
ACP 133 Name Forms

Item	Name Form	D & P	ACP 133	Notes	PICS Response
28	routingIndicatorNameForm	-	m		
29	sigintPLANameForm	-	m		
30	sIPLANameForm	-	m		
31	spotPLANameForm	-	m		
32	taskForcePLANameForm	-	m		
33	tenantPLANameForm	-	m		

Note 1: These name forms may be removed in a later edition of this ACP.

b. Table D-51 shows the name forms, defined in the 1997 edition of the Directory specifications, that shall be supported.

Table D-51
1997 Standard Name Forms

Item	Name Form	D	ACP 133	Notes	PICS Response
1	cRLDistPtNameForm	o	m		

d. Matching Rules

Table D-52 shows the matching rules, defined in the 1997 edition of the Directory specifications, that shall be supported.

Table D-52
1997 Standard Matching Rules

Item	Matching Rule	D	ACP 133	Notes	PICS Response
1	algorithmIdentifierMatch	o	m		
2	attributeCertificateMatch	o	m	see Note	
3	attributeIntegrityMatch	o	o		
4	certificateExactMatch	o	o		
5	certificateListExactMatch	o	m		
6	certificateListMatch	o	m	see Note	
7	certificateMatch	o	m	see Note	
8	certificatePairExactMatch	o	o		
9	certificatePairMatch	o	m		
10	readerAndKeyIDMatch	o	m		*

* Conditional on support of the encrypted variant of attributes as described in paragraph 408 of this ACP.

Note: Support for subelements of the matching rule is documented in the CMI CONOPS.

7. DUA Extensions

a. General

Table D-53 identifies use of the 1997 enhancements for security.

Table D-53
1997 Security Enhancements

Item No.	Operation	D	ACP 133			Predicate Name	Note	PICS Response
			Inter	Inter/ Mod	Adm			
1	Does the DUA support Signed Add Entry Enhancement?	o	o	o	m	signAdd97		
2	Does the DUA support Signed Remove Enhancement?	o	o	o	m	signRemove97		
3	Does the DUA support Signed Modify Entry Enhancement?	o	o	o	m	signModify97		
4	Does the DUA support Signed ModifyDN Enhancement?	o	o	o	m	signModDN97		
5	Does the DUA support Signed Errors	o	o	o	m	signErrors97		
6	Does the DUA support security parameters enhancement	o	o	o	m	securityParams97		

b. AddEntryResult

Table D-54 defines use of X.511 Signed Add Entry 1997 Enhancements. Note: This replaces ADY 41, A.4.3.3.8, item 2.

Table D-54
Signed Add Entry 1997 Enhancements
Prerequisite: signAdd97

Item No	Protocol Element	D	ACP 133	Note	PICS Response
2	AddEntryResult	m	m		
2.1	Null	c1	o		
2.2	information	c2	m		
2.2.1	OPTIONALLY-PROTECTED	c2	m	DIRQOP shall be Signed	
2.2.2	CommonResults	c2	m		
2.2.2.1	Security Parameters	c2	m	see Table D-59	

c1 If Not [signAdd97] then support of this feature is m else "o".
c2 If [signAdd97] then support of this feature is m else "-".

c. RemoveEntryResult

Table D-55 defines use of X.511 Signed Remove Entry 1997 Enhancements. Note: This replaces ADY 41, A.4.3.3.9, item 2.

Table D-55
Signed Remove Entry1997 Enhancements
Prerequisite: signRemove97

Item No	Protocol Element	D	ACP 133	Note	PICS Response
2	RemoveEntryResult	m	m		
2.1	Null	c1	o		
2.2	information	c2	m		
2.2.1	OPTIONALLY-PROTECTED	c2	m	DIRQOP shall be Signed	
2.2.2	CommonResults	c2	m		
2.2.2.1	Security Parameters	c2	m	see Table D-59	

c1 If Not [signRemove97] then support of this feature is m else "o".
c2 If [signRemove7] then support of this feature is m else "-".

d. ModifyEntryResult

Table D-56 defines use of X.511 Signed Modify Entry 1997 Enhancements. Note: This replaces ADY 41, A.4.3.3.10, item 2.

Table D-56
Signed Modify Entry 1997 Enhancements
Prerequisite: signModify97

Item No	Protocol Element	D	ACP 133	Note	PICS Response
2	ModifyEntryResult	m	m		
2.1	Null	c1	o		
2.2	information	c2	m		
2.2.1	OPTIONALLY-PROTECTED	c2	m	DIRQOP shall be Signed	
2.2.2	CommonResults	c2	m		
2.2.2.1	Security Parameters	c2	m	see Table D-59	

c1 If Not [signModify97] then support of this feature is m else "o"
c2 If [signModify97] then support of this feature is m else "-"

e. ModifyDNResult

Table D-57 defines use of X.511 Signed Modify DN 1997 Enhancements. Note: This replaces ADY 41, A.4.3.3.11, item 2.

Table D-57
Signed Remove Entry 1997 Enhancements
Prerequisite: signModDN97

Item No	Protocol Element	D	ACP 133	Note	PICS Response
2	ModifyDNResult	m	m		
2.1	Null	c1	o		
2.2	information	c2	m		
2.2.1	OPTIONALLY-PROTECTED	c2	m	DIRQOP shall be Signed	

Table D-57
Signed Remove Entry 1997 Enhancements
Prerequisite: signModDN97

Item No	Protocol Element	D	ACP 133	Note	PICS Response
2.2.2	CommonResults	c2	m		
2.2.2.1	Security Parameters	c2	m	see Table D-59	

c1: If Not [signModDN97] then support of this feature is m else "o".
c2: If [signModDN97] then support of this feature is m else "-".

f. Errors

Table D-58 defines use of X.511 Signed Errors 1997 Enhancements. Note: This updates Clause A.4.3.3.12 in ADY11 for signed errors and replaces A.4.3.3.12 in ADY41. Support for problem codes shall be as in ADY11 and ADY41. The following uses predicates defined in ADY11.

Table D-58
Signed Errors 1997 Enhancements
Prerequisite: signErrors97

Item No.	Protocol Element	D	ACP 133	Note	PICS Response
1	Abandoned	cn	c10		
1.0	OPTIONALLY-PROTECTED	c:o	m	DIRQOP shall be Signed	
1.1	CommonResults	c:m	m		
1.1.1	Security Parameters	c:m	m	see Table D-59	
1.2	algorithmIdentifier	c:m	m		
1.3	encrypted	c:m	m		
2	AbandonFailed	cn	c10		
2.0	OPTIONALLY-PROTECTED	c:o	m	DIRQOP shall be Signed	
2.1	problem	c:m	c:m	As in ADY11	
2.2	operation	c:m	c:m	As in ADY11	
2.3	CommonResults	c:m	m		
2.4.1	Security Parameters	c:m	m	see Table D-59	
2.5	algorithmIdentifier	c:m	m		
2.6	encrypted	c:m	m		
3	AttributeError	cn	c11		

Table D-58
Signed Errors 1997 Enhancements
Prerequisite: signErrors97

Item No.	Protocol Element	D	ACP 133	Note	PICS Response
3.0	OPTIONALLY-PROTECTED	c:o	m	DIRQOP shall be Signed	
3.1	object	c:m	c:m	As in ADY11	
3.2	problems	c:m	c:m	As in ADY11	
3.2.1	problem	c:m	c:m	As in ADY11	
3.3	type	c:m	c:m	As in ADY11	
3.4	value	c:o	c:m	As in ADY11	
3.5	CommonResults	c:m	m		
3.5.1	Security Parameters	c:m	m	see Table D-59	
3.6	algorithmIdentifier	c:m	m		
3.7	encrypted	c:m	m		
4	NameError	cn	c12		
4.0	OPTIONALLY-PROTECTED	c:o	m	DIRQOP shall be Signed	
4.1	problem	c:m	c:m	As in ADY11	
4.2	matched	c:m	c:m	As in ADY11	
4.3	CommonResults	c:m	m		
4.3.1	Security Parameters	c:m	m	see Table D-59	
4.4	algorithmIdentifier	c:m	m		
4.5	encrypted	c:m	m		
5	Referral	cn	i	See ADY12	
5.0	OPTIONALLY-PROTECTED	c:o	m	DIRQOP shall be Signed	
5.1	candidate	c:m	-	See ADY12	
5.2	CommonResults	c:m	m		
5.2.1	Security Parameters	c:m	m	see Table D-59	
5.3	algorithmIdentifier	c:m	m		
5.4	encrypted	c:m	m		
6	SecurityError	cn	c12		
6.0	OPTIONALLY-PROTECTED	c:o	m	DIRQOP shall be Signed	
6.1	problem	c:m	c:m	As in ADY11	
6.2	CommonResults	c:m	m		
6.2.1	Security Parameters	c:m	m	see Table D-59	
6.3	algorithmIdentifier	c:m	m		
6.4	encrypted	c:m	m		

Table D-58
Signed Errors 1997 Enhancements
Prerequisite: signErrors97

Item No.	Protocol Element	D	ACP 133	Note	PICS Response
7	ServiceError	cn	c12		
7.0	OPTIONALLY-PROTECTED	c:o	m	DIRQOP shall be Signed	
7.1	problem	c:m	c:m	As in ADY11	
7.2	CommonResults	c:m	m		
7.2.1	Security Parameters	c:m	m	see Table D-59	
7.3	algorithmIdentifier	c:m	m		
7.4	encrypted	c:m	m		
8	UpdateError	cn	c14		
8.0	OPTIONALLY-PROTECTED	c:o	m	DIRQOP shall be Signed	
8.1	problem	c:m	c:m	As in ADY11	
8.2	CommonResults	c:m	m		
8.2.1	Security Parameters	c:m	m	see Table D-59	
8.3	algorithmIdentifier	c:m	m		
8.4	encrypted	c:m	m		

c10: If [Abandon], then support of this feature is m else o.
c11: If [Read or Compare or Search or AddEntry or ModifyEntry], then support of this feature is m else o.
c12: If [Read or Compare or List or Search or AddEntry or RemoveEntry or ModifyEntry or ModifyDN], then support of this feature is m else o.
c13: If [pageresreq], then support of this feature is m else -.
c14: If [AddEntry or RemoveEntry or ModifyEntry or ModifyDN], then support of this feature is m else o.

g. Security Parameters

Table D-59 defines use of X.511 1997 Security Parameters. Note: This replaces clause A.4.3.3.22 in ADY 41.

Table D-59
Security Parameters including 1997 Enhancements
Prerequisite: securityParams97

Item No.	Protocol Element	D	P	ACP 133	Note	PICS Response
1	certification-path	m	m	m	see Note 1	
2	name	o	m	m		
3	time	o	m	m	see Note 2	
4	random	o	m	m	see Note 2	
5	target	o	m	o	see Note 3	
6	response	o	i	o		
7	operationCode	o	i	m	see Notes 4 & 5	
8	attribute CertificationPath	o	i	o		
9	errorProtection	o	i	o	see Note 3	
10	errorCode	o	i	m	see Notes 6 & 7	

Note 1: As specified for the Certificate Management Infrastructure (CMI).
Note 2: In request set as specified in X.511 '93 (need not be related in sequence to previous operations). In results or error this shall be set by the DSA and checked by the DUA to be the value of random in request argument plus 1 as specified in X.511 1997. The receiving DSA shall use time and "random" to ensure that an earlier request is not replayed.
Note 3: The policy shall define minimum levels for the target and error protection levels.
Note 4: This shall be the same as the code for the operation being carried out.
Note 5: A defect has been raised on the syntax for operationCode.
Note 6: This shall only be present if an error is being returned and shall be the same as the returned error code.
Note 7: A defect has been raised adding this errorCode to Security Parameters.

8. DSA Extensions

a. DAP

(1) Table D-60 identifies use of the 1997 enhancements for security.

Table D-60
1997 Enhancements

Item No.	Operation	D	ACP 133	Predicate Name	Note	PICS Response
1	Does the DSA support Signed Add Entry Enhancement?	o	m	signAdd97		
2	Does the DSA support Signed Remove Enhancement?	o	m	signRemove97		
3	Does the DSA support Signed Modify Entry Enhancement?	o	m	signModify97		
4	Does the DSA support Signed ModifyDN Enhancement?	o	m	signModDN97		
5	Does the DSA support Signed Errors		m	signErrors97		
6	Does the DSA support security parameters enhancement		m	securityParams97		

(2) The support for signed AddEntryResult shall be as defined in Table D-54. Note: This replaces ADY 42 A.4.3.3.8 item 2.

(3) The support for signed RemoveEntryResult shall be as defined in Table D-55. Note: This replaces ADY 42 A.4.3.3.9 item 2.

(4) The support for signed ModifyEntryResult shall be as defined in Table D-56. Note: This replaces ADY 42 A.4.3.3.10 item 2.

(5) The support for signed ModifyDNResult shall be as defined in Table D-57. Note: This replaces ADY 42 A.4.3.3.10 item 2.

(6) The support for signed Errors shall be as defined in Table D-58. Note: This updates ADY21 Clause A.4.3.3.12 and ADY 42 A.4.3.3.12. Support for problem codes shall be as in ADY21 and ADY42.

(7) The support of the security parameters field shall be as defined in Table D-59. Note: This replaces clause A.4.3.3.22 in ADY 42.

b. DSP

(1) Table D-61 identifies use of the 1997 enhancements for security.

Table D-61
1997 Enhancements

Item No.	Operation	D	ACP 133	Predicate Name	Note	PICS Response
1	Does the DSA support Signed Errors	o	m	signErrors97		

(2) The support for signed errors shall be as defined in Table D-58 with the exception that item 5 (Referral) is replaced with DSAReferral in Table D-62. Note: This replaces Clause A.4.3.5 in ADY22 for signed errors.

Table D-62
Signed Errors 1997 Enhancements
Prerequisite: signErrors97

Item No.	Protocol Element	D	ACP 133	Note	PICS Response
5	DSAReferral	cn	i	See ADY12	
5.0	OPTIONALLY-PROTECTED	c:o	m	DIRQOP shall be Signed	
5.1	continuationPrefix			See ADY12	
5.2	contextPrefix	c:m	-	See ADY12	
5.3	CommonResults	c:m	m		
5.3.1	Security Parameters	c:m	m	see Table D-59	

Table D-62
Signed Errors 1997 Enhancements
Prerequisite: signErrors97

Item No.	Protocol Element	D	ACP 133	Note	PICS Response
5.4	algorithmIdentifier	c:m	m		
5.5	encrypted	c:m	m		

(3) The support of the security parameters field shall be as defined in Table D-59. Note: This replaces clause A.7.2 in ADY 43.

c. DISP

(1) Table D-63 identifies use of the 1997 enhancements for security.

Table D-63
1997 Enhancements

Item No.	Operation	D	ACP 133	Predicate Name	Note	PICS Response
1	Does the DSA support Signed shadow result Enhancement?	o	m	signShadRes97		
2	Does the DSA support Signed Errors		m	signErrors97		
3	Does the DSA support security parameters enhancement		m	securityParams97		

(2) Table D-64 defines use of Signed Shadow 1997 enhancement. Note: This replaces ADY43, A.6.1.2.3, item 12.

Table D-64
Signed Shadow 1997 Enhancements
Prerequisite: signShadRes97

Item No.	Protocol Element	D	ACP 133	Note	PICS Response
12	xxx-result	m	m		
12.1	Null	c1	o		
12.2	information	c2	m		
12.2.1	OPTIONALLY-PROTECTED	c2	m	DIRQOP shall be Signed	
12.2.2	CommonResults	c2	m		
12.2.2.1	Security Parameters	c2	m	see Table D-59	

c1 If Not [signShadRes97], then support of this feature is m else "o".
c2 If [signShadRes97], then support of this feature is m else "-".

(3) Table D-65 defines use of X.525 Signed Errors 1997 Enhancements. Note: This replaces ADY51, A.4.3.6 for signed errors.

Table D-65
Signed Errors 1997 Enhancements
Prerequisite: signErrors97

Item No.	Protocol Element	D	ACP 133	Note	PICS Response
1	shadowError	m	m	As in ADY51	
2	OPTIONALLY-PROTECTED	c:o	m	DIRQOP shall be Signed	
3	problem		m	As in ADY51	
4	lastUpdate	o	m	As in ADY51	
5	updateWindow	o	m	As in ADY51	
3	CommonResults	c:m	m		
4	Security Parameters	c:m	m	see Table D-59	
5	algorithmIdentifier	c:m	m		
6	encrypted	c:m	m		

(4) The support of the security parameters field shall be as defined in Table D-59. Note: This replaces use of security parameters in ADY 51, clauses A.4.3.3, A.4.3.4 and A.4.3.5.

9. Schema Extensions

Table D-66 summarizes the requirement to support the Universal Character String Transformation Format 8 (UTF-8) encoding of the ISO/IEC 10646 Character Set. This string type will be usable wherever the Directory String type is used, e.g., Distinguished name, pubic key certificates. (PrintableString and TeletexString are required to be supported by the X.500 standard.) A proposed amendment to X.519 and X.520 to add a choice of UTF-8 to the definition of DirectoryString is expected to be approved in 1999.

Table D-66
Directory String Support

Item	Matching Rule	D	ACP 133	Notes	PICS Response
1	Does the DSA Support UTF-8 strings?	o	m		

10. Corrigenda not included in ISPs

[Ed.: To be supplied.]

APPENDIX 1 TO ANNEX D

DEFECT REPORT FORM

1. Defect Report Number:
   Title: Use of Operation and Error Code in Security Parameters

2. Source:

3. Addressed to:

   (a)

   (b)

4. Date circulated by WG Secretariat:

5. Deadline for Response from Editor:

6. Defect Report Concerning:

   ITU-T X.511 (1997) | ISO/IEC 9594-3:1997

7. Qualifier:

   Error and Omission

8. References in Document:

   Clause 7.10

9. Nature of Defect:

   (a) The syntax of operationCode in Security Parameters is currently defined as an Object Identifier. However, Remote Operation Service (ROS) Operation Codes may be either Integer or Object Identifier and currently all the X.500 operation codes are defined as Integers.

   (b) Since error codes are not protected a similar attack can occur on error responses to the attack on operation codes. Where both a successful response and error contains signed Security Parameters with no extra parameters (e.g. Modify Response and Abandon Error), the unprotected part of a PDU may be altered to change an error to success without detection.

10. Solution Proposed by the Source:

In clause 7.10:

(a) Replace syntax for operationCode in SecurityParameters to be:

operationCode [6] Code OPTIONAL

Code should be imported from:
Remote-Operations-Information-Objects {
joint-iso-ccitt remote-operations(4) informationObjects(5) version1(0) }

and in the paragraph describing **operationCode** delete "object identifier". Also, at end of paragraph change "or results" to ", results or errors".

b) Add to the SecurityParameters syntax:

errorCode [9] Code OPTIONAL

and add the following description:

The **errorCode** is used to secure the error code where an error is returned in response to an operation.

11. Editor's Response:

ANNEX E

EXAMPLE SHADOWING AGREEMENT

Table E-1 Example Shadowing Agreement Checklist	
Legend:	
SD	indicates the shadow Supplier DSA administrator must provide information/initial agreement
CD	indicates the shadow Consumer DSA administrator must provide information/initial agreement
MD	indicates the Master DSA administrator must initial agreement
DM	indicates the Directory Services Manager must initial agreement
Supplier DSA (SD)	
DSA Name:	
DSA location (including building & room number):	
Communications address:	
Primary Point of Contact name:	
Commercial telephone number:	
Military telephone number:	
E-mail address:	
Postal address:	
Secondary Point of Contact name:	
Commercial telephone number:	
Military telephone number:	
E-mail address:	
Postal address:	
Tertiary Point of Contact (24 hours, 7 days a week):	
Commercial telephone number:	
Military telephone number:	
Consumer DSA (CD)	
DSA Name:	
DSA location (including building & room number):	
Communications address:	
Primary Point of Contact name:	
Commercial telephone number:	
Military telephone number:	
E-mail address:	

Table E-1 Example Shadowing Agreement Checklist
Postal address:
Secondary Point of Contact name:
Commercial telephone number:
Military telephone number:
E-mail address:
Postal address:
Tertiary Point of Contact (24 hours, 7 days a week):
Commercial telephone number:
Military telephone number:
Agreements
1.(SD)____ (CD)____ Both DSAs involved in this agreement are ACP 133 compliant DSAs.
2.(SD)____ (CD)____ Both DSAs involved in this agreement operate under compatible security policies.
3. If the consumer DSA is to act as a backup to the supplier DSA, this section must be completed. (CD)____ The consumer DSA understands and agrees that if the supplier DSA fails or is unavailable, that the consumer DSA must support the supplier DSA agent's accesses. (SD)____ During a normal 8-hour working period the supplier DSA unit of replication is accessed approximately _____ times. During the worst case 8-hour period the unit of replication has or may experience approximately _____ accesses.

Table E-1

Example Shadowing Agreement Checklist

4. X.500 standard shadowing specifications

(SD)_____ (CD)_____ The Unit of Replication is:

Area Specification:

Context Prefix: _____

Subtree Specification:

Base: _____

Chop:_____

Filter (object classes): _____

Attribute Selection:

All attributes_____ or

Include attributes: _____

_____

Exclude attributes: _____

Include knowledge held of _____master and/or_____shadow naming contexts.

Update Mode: _____

Master: _____

Secondary Shadows: _____

_____

5.(SD)____ The supplier DSA information area to be replicated contains _____ kbytes (includes a 30% growth factor). If the replicated area grows beyond this size, the supplier DSA agrees to immediately re-negotiate to amend this agreement.

(CD)____ The consumer DSA acknowledges the size of the shadow copy to be held.

6.(SD)____ During a normal 8-hour working period the supplier DSA unit of replication is modified (entries added, deleted, changed) approximately _____ times.

(CD)____ The consumer DSA acknowledges the impact of the modifications.

7.(SD)____ The supplier DSA was, in the last 90 days if possible, on-line and accessible ____% of the time.

(CD)____ The consumer DSA was, in the last 90 days if possible, on-line and accessible ____% of the time.

(SD)____ (CD)____ The supplier DSA and consumer DSA acknowledge the reliability rate.

Table E-1 Example Shadowing Agreement Checklist
8.(SD)____(CD)____ The supplier and consumer DSAs agree to immediately notify each other in the event either DSA fails or is otherwise unavailable for service.
9.(SD)____(CD)____ The supplier and consumer DSAs (points of contact) agree this shadowing agreement shall go into effect at _____ UTC and remain in effect until _____ UTC.
10.(SD)____(CD)____ This agreement may be terminated by either the consumer or supplier DSAs if terms and conditions in this agreement are modified without re-negotiation.
11.(CD)____ The consumer DSA agrees to provide 30 days notification, if for any reason the consumer DSA will be unable to fulfill this agreement. (SD) ____ The supplier DSA agrees to provide 30 days notification, if for any reason the supplier DSA will be unable to fulfill this agreement.
12.(CD)____ Further constraints/conditions of the supplier DSA: _____ _____ _____ (SD)____ Further constraints/conditions of the consumer DSA: _____ _____ _____
13.(SD)____(CD)____ If update is to occur upon changes, the maximum period over which changes are accumulated before the shadowing is done is _____.
14.(DM)____ The Directory Services Manager agrees that this agreement is consistent with policy and that the topology involved is consistent with replication policy regarding the best choice for minimizing hops and single point of failure avoidance.
15.(MD)____ If this agreement is for secondary shadowing, the Master DSA administrator agrees that the agreement is consistent with the information owner's policy.

Table E-1

Example Shadowing Agreement Checklist

16. Protection provided to shadowed information

Type of Authentication

None____

Simple____

Strong____

Variable (as per ACI shadowed) ____

Type of Access Control

Basic____

Simplified____

Rule-Based____

General Protection (for read access);

restricted to these users: _____

(CD)_____The consumer will apply ACI that is shadowed with the unit of replication.

17. When a shadowing agreement is terminated, the shadow consumer agrees to remove the shadowed information from the consumer DSA within time period_____.

18. Auditing that will be done by the consumer on shadowed information and details on access to and archive of audit data.

Note that indicating that secondary shadowing of the subject information can be performed does not preclude the necessity for each secondary shadow being (part of) the subject of a (secondary) shadowing agreement.

ANNEX F

EXAMPLE SERVICE LEVEL AGREEMENT

SERVICE LEVEL AGREEMENT

BETWEEN THE

< NAMES OF ORGANIZATIONS>

FOR THE

PROVISION OF DIRECTORY SERVICES

VERSION HISTORY

	Section	**Issue**	**Date of Issue**	**Remarks**
Main Document	Service Level Agreement			
Appendix A	Service Profiles			
Appendix B	Management and Reporting Criteria			
Appendix C	Management Points of Contact			
Appendix D	Finance			

DISTRIBUTION

COPY NUMBER	HOLDER	LOCATION
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		
11		

CONTENTS

DEFINITIONS

Services	The provision of planning, procurement, implementation, change control, task co-ordination, project management, configuration management, maintenance, security, documentation, operator services, quality control, and financial management of <assets> within the <organization> area of responsibility.
Customer	The organization receiving directory services from the <service provider>. The Customer will be represented by a nominated person for each Customer site representing all users of services.
SLA Review Meeting	The SLA Review Meeting is held to discuss and approve any changes required to the SLA document. Chaired by <as appropriate>.
Project Review Board	The Project Review Board (PRB) meets to discuss policy and strategic level project issues. It is chaired by <as appropriate>.

GLOSSARY

1. ACP Allied Communication Publication

REFERENCES

1. ACP 133 version < >

INTRODUCTION

PURPOSE OF THIS DOCUMENT

1. This section gives details of the participating governments. It gives any background to the requirement for the establishment of electronic directory services. It mentions that the SLA exists for the further cooperation relating to the relating to the establishment, assignment, utilization, practices and payment for electronic directory services shared or provided between the participating organizations.

SCOPE

2. The scope covers the provision of electronic directory services by giving a brief, high level description of the services being provided, information regarding the provision of resources and any relevant instructions and constraints. Also covered is amendment or cancellation and its effect on the SLA.

RESPONSIBILITIES

3. Identifies those parties/authorities responsible for the implementation of the agreement. It details the levels at which coordination between the parties can take place. The specific technical details for the levels of service, procedures and practices, restoration, leasing and postal and communications addresses and funding are to be included in Appendices referenced from this section.

IMPLEMENTATION

4. Each party will have responsibility for its own directory systems, including the procurement and maintenance of equipment and services. Working level details will need to be outlined within appendices to the document and should include, where necessary, details of the responsibilities and tasks one nation may offer another nation in setting up the service. It should designate any project planning time scales.

SERVICES TO BE PROVIDED

5. Service Profiles - The Provider will meet the Customer-specific requirements detailed in Appendix A to this SLA.

6. Management and Reporting Criteria - The Provider will deal with fault conditions in accordance with Appendix B.

7. Management Points of Contact - Points of contact at various levels in the management chain are given in Appendix C.

FUNDING

8. This section makes statements about who has financial responsibility for different parts of the system. As in establishing a bilateral agreement between two nations, both nations will benefit from a mutual exchange of information which may imply that there would be no costs levied for the provision of the service. Each party would normally bear the costs of its own operations and maintenance. Also included would be any reimbursements of costs. An appendix giving the precise details of costs would be referenced.

SECURITY

9. Details are to be given of the classification of the directory service and the security mechanisms to be implemented.

RELEASE OF INFORMATION

10. The rules of release of one nation's information to others, including members of its own Armed Forces, public and press. The mechanisms to undertake the safeguarding of protectively marked material as well as the handling of unclassified material.

WAIVER OF CLAIMS

11. Statements on waiver of claims resulting from loss, damage or failure of equipment.

ARBITRATION AND DISPUTES

12. A statement constraining the parties to resolve any disagreements between themselves and limiting the level of escalation.

ENTRY INTO FORCE, TERMINATION, AND REVIEW

13. Statements covering the bringing into force of the agreement, its length of validity, notice of termination and the period of review for the agreement are to be given, including any requirement for review meetings.

AUTHORITY FOR AGREEMENT

Signed for and on behalf of < responsible initiating authority>

Date: _____ Signature: _____

<Rank/Name/Position>

Signed for and on behalf of the <other party>

Date: _____ Signature: _____

<Rank/Name/Position>

APPENDIX A - SERVICE PROFILES

1. The tables below define the service profiles available for each of the provided services.

DIRECTORY SERVICE (for example)

SERVICE ATTRIBUTES	SERVICE OPTION No.	SERVICE OPTION DESCRIPTION
FEATURES	1a	
	1b	
SECURITY	2a	UNCLASSIFIED
	2b	RESTRICTED
	2c	SECRET
MANAGEMENT	3a	No Control or Monitoring
	3b	Central Control and Monitoring
	3c	
	3d	Local control only
SURVIVABILITY	4a	Standard
	4b	Physical security
	4c	Blast protected
	4d	EMP protected
	4e	Route Diversity
INTERFACES	6a	
	6b	
PERFORMANCE	7	
PERFORMANCE (Site Service Availability measured over 1 year)	7a	x%
	7b	x%
PERFORMANCE (Grade of Service)	7d	
SYNCHRONIZA-TION		
MAINTENANCE	9a	Next working day attention
	9b	4 hour maximum time to respond 0800-1700 Mon to Fri
	9c	4 hour maximum time to respond at any time

	9d	4 hour mean time to repair at any time

CONFIGURATION DETAILS

2. This section shall include directory configuration details covering:

- Naming Context
- Knowledge information
- Shadowing agreements
- Secondary Shadowing authorizations
- Underlying protocol stack
- Replication agreements

3. Protocol Profiles are required for DAP, DISP, DOP, and DSP.

ACCESS CONTROL PROFILES

4. Any national directory system contains national preferences for Access Control. An agreed Access Control Infrastructure will need to be developed and the profiles recorded.

5. A key and certificate management regime will be required if the directory system may require its interfaces (DAP, DSP, DISP and DOP, if used), to be fully authenticated.

ADMINISTRATIVE PROFILES

6. Profiles are required for ADUAs.

7. An agreement will need to be made on clock synchronization.

APPENDIX B - MANAGEMENT AND REPORTING CRITERIA

1. This appendix details the Customer-specific requirements of service management and reporting.

FAULT REPORTING AND HELP SERVICES

2. When a fault condition occurs, the Customer is first to check that it has not been caused by the Customer's equipment. Once satisfied that this is not the case, the Customer will submit a fault report to the service provider.

3. A Help desk will be established to provide the first point of customer contact for service queries and will be able to answer both technical and procedural questions.

SERVICE RESTORATION

4. Following a fault, the Provider will ensure that the service is restored within the <defined> time scales. A service will not be considered to be restored until positive confirmation has been obtained from the Customer. During service restoration the Provider will provide the Customer reporting the fault with progress information.

5. The specified restoration time is to start from the receipt of the fault report by the help desk, unless the fault is initially detected by the Provider, in which case the restoration time is to start from the time of detection.

6. The Provider will provide the Customer reporting the fault with the following information during fault restoration:

- Within 30 minutes of the report of a fault, provide an estimate of the restoration time.

- If it becomes apparent that the estimated restoration time will not be met, immediately advise the Customer accordingly, and as soon as possible thereafter advise the Customer of the new forecast restoration time.

7. If the Provider fails to meet the restoration time for a service, as specified in Appendix A, he is to take the following actions:

- Inform the Customer immediately, agree the update rate with the Customer, and provide a new estimated restoration time.

- Formally record the failure to meet the restoration time, and provide a written report to the Customer.

- The Help Desk will, on request from a Customer, provide details of contacts through whom the requirement for fault restoration can be escalated.

REAL TIME MONITORING

8. The Provider will monitor and analyze performance criteria in real time to identify shortfalls against Appendix A and manage the system proactively by:

- Informing the Customer of faults that Customers may not be aware of but which may affect Customer services.

- Offering advice on alternative services under fault conditions.

INVESTIGATIONS AND REPORTING

9. The Provider will provide the Customer with the following routine reports:

- A monthly summary of actual performance against the requirements contained within this agreement and actions in hand to correct any deficiencies.

- A quarterly report covering technical, operational <and financial performance>.

- An annual report covering audits and any service development plans produced by the contractors.

10. The Provider will undertake investigations and provide the Customer with special reports, on request, under the following circumstances:

- Persistent failure to meet one or more performance targets.

- Major loss of service or catastrophic failure.

SCHEDULED LOSS OF SERVICE

11. The Provider will give the Customer one calendar month written notice of any proposed scheduled loss of service. Any variation from this is to be agreed on an exceptional basis only. The timing, extent and duration of any such loss of service is to be negotiated and agreed by the Provider and the Customer on a case by case basis.

SERVICE PROVISION

12. The Provider will supply a service in the planning and implementation of minor and major projects. The Provider is to meet, from receipt of the requirement, the specified time scales for the three categories as shown below:

Category	Time scale
Operational	<Two days> Earlier time scale, if achievable, to be agreed within 24 hours of receipt
Priority	<Five days> Earlier time scale, if achievable, to be agreed within 24 hours of receipt
Normal (baseline)	

13. Moves and changes will be delivered as follows:

- 85 % of scheduled site housekeeping routines completed within one day of agreed scheduled time.
- 85 % of system software controlled moves and changes completed within one working day.
- <> % of on site small physical moves and changes completed within <> working days of receipt of request.

DOCUMENTATION

14. The Provider will issue to the Customer sufficient copies of documents to allow efficient use of the services provided.

MEETINGS

15. <As Appropriate>

APPENDIX C - MANAGEMENT POINTS OF CONTACT

The tables below show the normal levels at which contact is made:

Hour by Hour Management

Service Provider	Customer
Help Desks:	

System Supervisor:	

Policy and Management Escalation

Service Provider	**Customer**
Action Office:	

APPENDIX D - FINANCE

1. This appendix should contain details of the financial arrangements between the parties, including costs incurred and any accrued credits or liabilities.

2. Each party would normally bear the costs of operation and maintenance of its own directory infrastructure.

ANNEX G

ABBREVIATIONS

The following abbreviations and acronyms are used in this ACP:

ACDF	Access Control Decision Function
ACI	Access Control Information
ACP	Allied Communication Publication
ACSE	Association Control Service Element
ADUA	Administrative Directory User Agent
ADY	1993 Directory Application Profile
AIG	Address Indicator Group
AL	Address List
AMH	Allied Message Handling
APP	Allied Publications Procedures
ASCII	American Standard Code for Information Interchange
ASN.1	Abstract Syntax Notation One
AU	Australia
AUTODIN	Automatic Digital Network
BAC	Basic Access Control
C	Country
CA	Canada; Certification Authority
CAD	Collective Address Designator
CCEB	Combined Communications Electronics Board
CCITT	The International Telegraph and Telephone Consultative Committee

CMI	Certificate Management Infrastructure
CMIP	Common Management Information Protocol
CN	Common Name
CONOPS	Concept of Operations
COSINE	Organization for Cooperation for OSI Networking in Europe
COTS	Commercial Off-the-Shelf
CPS	Certificate Practice Statement
CRL	Certificate Revocation List
CSP	Common Security Protocol
CTF	Combined Task Force
CULR	Common Upper Layer Requirements
DAG	DSSCS Address Group
DAP	Directory Access Protocol
DFTS	Defense Fixed Telecommunications Service
DIB	Directory Information Base
DISP	Directory Information Shadowing Protocol
DIT	Directory Information Tree
DL	Distribution List
DMD	Directory Management Domain
DN	Distinguished Name
DODAAC	Department of Defense Activity Accounting Code
DOP	Directory Operational Binding Management Protocol
DSA	Directory System Agent
DSE	DSA-specific entry

DSN	Defense Switched Network
DSP	Directory System Protocol
DSSCS	Defense Special Security Communications System
DUA	Directory User Agent
EDI	Electronic Data Interchange
EIT	Encoded Information Type
E-MAIL	Electronic Mail
EOS	Elements of Service
FDY	1993 Directory Interchange Format and Representation Profile
FLDSA	First-level DSA
G3	Group 3 Facsimile
G4	Group 4 Facsimile
GENSER	General Service
GHP	Gateway Handling Policy
HOB	Hierarchical Operational Binding
HQ	Headquarters
IA5	International Alphabet Number 5
IBAC	Identity-based Access Control
IC	Intelligence Community
IEC	International Electrotechnical Commission
ILS	Integrated Logistics Support
ISDN	Integrated Services Digital Network
ISME	International Subject Matter Experts
ISO	International Organization for Standardization

ISP	International Standardized Profile
ITU-T	International Telecommunication Union-Telecommunication Standardization Sector
JANAP	Joint Army, Navy, Air Force Procedure
L	Locality
LCC	Local Control Center
LEP	List of Effective Pages
LMF	Language and Media Format
LOP	Letter of Promulgation
MCS	Message Conversion System
MHS	Message Handling System
MIB	Management Information Base
MLA	Mail List Agent
MMHS	Military Message Handling System
MMUA	Military Messaging User Agent
MS	Message Store
MTA	Message Transfer Agent
MTBF	Mean Time Before Failure
MTS	Message Transfer System
MTTR	Mean Time to Repair
NASIS	NATO Subject Indicator System
NATO	North Atlantic Treaty Organization
NAVCOMPARS	Naval Communications Processing and Routing System
NZ	New Zealand

O/R, OR	Originator/Recipient
O	Organization
OSI	Open Systems Interconnection
OU	Organizational Unit
P2	Interpersonal Messaging - 1984 Content Type
P22	Interpersonal Messaging - 1988 Content Type
P772	Military Messaging Content Type
PACOM	Pacific Command
PICS	Protocol Implementation Conformance Statement
PKI	Public Key Infrastructure
PLA	Plain Language Address
PRB	Project Review Board
PRMD	Private Management Domain
PSTN	Public Switched Telephone Network
R	GENSER Community
RAN	Release Authority Name
RBAC	Rule-Based Access Control
RDN	Relative Distinguished Name
RFC	Request for Comments
RHOB	Relevant Hierarchical Operational Binding
RI	Routing Indicator
ROSE	Remote Operations Service Element
RTSE	Reliable Transfer Service Element
S/MIME	Secure/Multimedia Internet Mail Extensions

SA	Signal Address
SAC	Simplified Access Control
SDN	Secure Data Network
SHD	Special Handling Designator
SI	Special Intelligence
SIC	Subject Indicator Code
SIGAD	SIGINT Address
SIGINT	Signal Intelligence
SLA	Service Level Agreement
SMIB	Security Management Information Base
SMA	Signal Message Address
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
STANAG	Standardization Agreement
STU	Secure Telephone Unit
TARE	Telegraph Automatic Relay Equipment
TCC	Transmission Control Code
TCCG	Transmission Control Code Group
TR	Technical Report
TRC	Transmission Release Code
TSGCE	Tri-Service Group of Communications and Electronics
UA	User Agent
UK	United Kingdom
UKM	User Key Material

US	United States
USMCEB	United States Military Communications-Electronics Board
UTC	Universal Coordinated Time
Y	SI Community

LIST OF EFFECTIVE PAGES

Subject Matter	Page Numbers	Change in Effect
Title Page	I (Reverse Blank)	Edition B
Foreword	III (Reverse Blank)	Edition B
Letter of Promulgation	V (Reverse Blank)	Edition B
Record of Changes and Corrections	VII to XVI	Edition B
Record of Pages Checked	XVII, XVIII	Edition B
Table of Contents	XIX to XXIV	Edition B
Chapter 1	1-1 to 1-6	Edition B
Chapter 2	2-1 to 2-20	Edition B
Chapter 3	3-1 to 3-44	Edition B
Chapter 4	4-1 to 4-12	Edition B
Chapter 5	5-1 to 5-4	Edition B
Annex A	A-1 to A-6	Edition B
Annex B	B-i to B-xvi, B-1 to B-170	Edition B
Annex C	C-1 to C-18	Edition B
Annex D	D-i to D-iv, D-1 to D-52	Edition B
Annex E	E-1 to E-6	Edition B
Annex F	F-1 to F-14	Edition B
Annex G	G-1 to G-8	Edition B
List of Effective Pages	LEP-1 to LEP-2	Edition B